PERSEREC

Technical Report 04-2
April 2004

Reciprocity: A Progress Report

Katherine L. Herbig
Northrop Grumman Mission Systems

Peter R. Nelson
Northrop Grumman Mission Systems Consultant

Research Supported by
Personnel Security Managers' Research Program

Research Conducted by
Defense Personnel Security Research Center

Technical Report 04-2 **April 2004**

Reciprocity: A Progress Report

Katherine L. Herbig
Northrop Grumman Mission Systems

Peter R. Nelson
Northrop Grumman Mission Systems Consultant

Released by
James A. Riedel
Director

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-04-2004	Technical	27-04-1953 to 30-10-2003

4. TITLE AND SUBTITLE

RECIPROCITY: A PROGRESS REPORT

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Katherine L. Herbig
Peter R. Nelson

5d. PROJECT NUMBER
VS-02-3

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

8. PERFORMING ORGANIZATION REPORT NUMBER

TR 04-2

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Personnel Security Managers' Research Program
Plaza A Building
Washington, DC 20505

10. SPONSOR/MONITOR'S ACRONYM(S)

PSMRP

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

A study was conducted evaluating the degree and types of personnel security reciprocity in effect between agencies of the executive branch and their contractors. Interviews with security directors and staff at 14 federal agencies and 5 contractor companies produced data suggesting that reciprocity has improved since 1995 but that it is still partial. Findings report areas in which reciprocity generally works (visits, community badge, updating the SF-86); areas in which it works sometimes (electronic databases, reviews of prior investigations, polygraph); and areas in which it seldom works (conversions, industrial contractors, SAPs, suitability vs. security). Reasons for lack of reciprocity are discussed, and five options for action are outlined.

15. SUBJECT TERMS

Reciprocity Personnel Security Background Investigations Adjudication
Executive Order 12968 Access to Classified Information History of Reciprocity Policy

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
UNCLASSIFIED					James A. Riedel, Director
a. REPORT	b. ABSTRACT	c. THIS PAGE		74	19b. TELEPHONE NUMBER *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			831-657-3000

Preface

Reciprocity has been a goal of the personnel security system for at least a decade. The expectation is that standardized national policies and procedures should result in uniform personnel security products that are interchangeable regardless of the issuing agency. The policy as stated in National Security Directive 63 is that investigations and clearance eligibility determinations that meet national scope and standards are transferable and, according to Executive Order 12968, "shall be mutually and reciprocally accepted by all agencies." The objective of this study was to ascertain the impact of reciprocity on current personnel security practices across the executive branch. Reciprocity touches a broad cross-section of personnel and agencies in the Defense, Intelligence, and Energy communities. It involves government civilians, members of the military, and employees of industrial contractors who fall under the National Industrial Security Program. Because of the breadth of the issue, the research effort in this study focused on gathering data through interviews with representatives from the numerous constituencies and analyzing common themes and concerns that were expressed.

This research was sponsored by the Personnel Security Managers' Research Program, whose interests spanned the Intelligence and Defense communities. It documents the progress that has been achieved in reciprocity since 1997, and it also documents areas in which progress has been slow. It outlines for the consideration of policymakers various options for action on reciprocity. This study will be useful and of interest to individuals in the executive branch of the federal government whose personnel security policies and procedures are subject to the current policy of reciprocity.

James A. Riedel
Director

Executive Summary

Introduction

Reciprocity is a policy that requires acceptance of equivalent personnel security clearances and accesses across the executive branch of the federal government. Authority for the current reciprocity policy is found in an executive order issued in 1995 by President William J. Clinton: Executive Order (E.O.) 12968, *Access to Classified Information.* Two years later the President approved uniform guidelines, mandated in the executive order, in the *Adjudicative Guidelines and Investigative Standards.* They have been implemented throughout the executive branch. The Personnel Security Managers' Research Group (PSMRP) tasked the Defense Personnel Security Research Center (PERSEREC) in 2002 to conduct research on reciprocity that would evaluate the policy and identify potential options for action.

Background

A thorough literature review was undertaken in relevant government policy documents, studies, audits, and working group reports to document the history of the current reciprocity policy. This section traces the evolution, particularly in the Department of Defense (DoD), from localized to more consolidated functions in the three activities that define personnel security: background investigation, adjudication, and maintenance of accurate records on the current status of an individual's accesses. It also describes the development of the reciprocity policy itself. We argue that until the basis for a certain level of standardization was achieved, through advances such as the Single Scope Background Investigation (SSBI), partial consolidation of adjudication within DoD in 1993, and the increasing reliance on electronic databases for records maintenance, reciprocity across the various agencies and military departments of the executive branch could not be expected. With these and other milestones in place by 1995, the long-discussed policy of reciprocity was mandated in E.O. 12968.

Approach

In order to gather information with which to evaluate reciprocity, we conducted interviews with security directors and their staff members at 14 government agencies and five defense contractor companies. Semi-structured interviews were used based on a protocol developed to explore the major issues of reciprocity. During the interviews, informants were encouraged to expand on issues as appropriate and to apply questions to the particular circumstances and needs of their agencies. This produced narrative data that was organized by topic. By speaking with a wide variety of individuals who were conversant with the workings and failings of reciprocity, we learned that some aspects of the policy are working out better than others.

Findings

According to interview respondents, among the interactions in which reciprocity has been improved and now works quite well were visits between agencies, the community badge, and routine updating of the form that initiates a background investigation, the "Questionnaire for

National Security Positions," also known as the SF-86, or in electronic form as the "Electronic Personnel Security Questionnaire," the EPSQ. Visit request and access certification systems are widely familiar, and people look forward to further efficiencies from the networking of electronic databases. The community badge has improved visit reciprocity within the 13 agencies of the Intelligence Community (IC) because typically it is recognized across agencies without the need to pass certifications for each visit. Most agencies reported that they routinely require an updated SF-86 from applicants for access longer than a visit. Under current policy, agencies are responsible to assure themselves that no security-relevant issues have appeared in applicants' lives since their most recent background investigation. Thus it is widely accepted that requiring an updated form since the previous background investigation is prudent and necessary. This allows an agency to do further investigation if security-relevant issues emerge. However, procedures for updating this form are hardly standardized across agencies, and updating currently takes time and causes delays that the framers of reciprocity policy sought to avoid. Respondents hoped that adoption of the SF-86C form, which allows an annual electronic update of one's SF-86 on file in order to keep the information current, would improve the efficiency of what they saw as a necessary procedure.

From the interviews it seemed that certain procedures that require reciprocity have improved since E.O. 12968 but still fall short of actual reciprocity. Three of these areas were: initiatives to expand the use of electronic databases; the review of the files of prior background investigations; and the reciprocal acceptance of the results of polygraph tests.

Respondents strongly agreed that reciprocity depends on access to up-to-date and accurate information about the following: the current status of an individual's clearances and accesses, type and date of background investigations, and an explanation of exceptions, issues, and the adjudicative reasoning that was followed. They also agreed that although this ideal does not yet exist, progress was being made toward it. The networking being done to link or exchange some types of records between various databases being developed was eagerly awaited by most respondents. Many expected that DoD's Joint Personnel Adjudication System (JPAS), which will document adjudication decisions made across DoD agencies and departments, would facilitate reciprocity by offering timely and convenient access to these data for agencies across the government checking on a person's clearance status. The recent creation of data links between JPAS and the Clearance Verification System (CVS), which has been developed by the Office of Personnel Management (OPM), further enhances the ability to quickly check a person's status in an electronic file. The more convenient and accurate these tools for records maintenance and verification become, the more they will contribute to reciprocity.

Although reciprocity policy discourages redundant investigation and re-adjudication, more than half of respondents among executive agencies said they routinely request prior background investigations for review. The reasons given for these reviews clustered around several related concerns. Respondents typically assumed that the particular demands of their own agencies required extra caution. Some felt that because these demands were above and beyond the norm, prudence dictated a review of the investigative file in order to meet their agency's security responsibilities. There was general awareness that policy and regulations do not allow re-adjudication of a past investigation without good reason, that is, unless new security-relevant issues have arisen since the last adjudication. However, for most respondents, the need to check

for new issues since the last investigation justified reviewing recent investigative files. This step of requesting and reviewing files of previous investigations added several weeks or even months to the process of personnel transferring between agencies, and it was this type of delay that the framers of reciprocity policy sought to mitigate.

There are differences of opinion among executive branch agencies about the reliability of polygraph testing, and these differences prevent mandating reciprocity of polygraph testing across all federal agencies. Instead, agencies in the IC that do incorporate the polygraph into their security procedures work reciprocally with one another based on a Memorandum of Agreement (MOA) that was reached in 1998. Information from respondents suggested that IC agencies were often willing to accept a favorable polygraph from another IC agency—and not to insist that the applicant take another test—but that this acceptance depended on which agency had performed the test, the scope of the test, and how recently it had been taken. IC agencies vary among themselves about the scope and recency of previous polygraph testing they require before they demand that an individual take another test given by their own agency.

Several common procedures in personnel security serve to put people to work more quickly, but these procedures also pose problems for reciprocity policy. Interim security clearances and accesses are issued by many agencies while normal background investigation and adjudication procedures are still underway, as long as initial records checks support this shortcut. E.O. 12968 recognizes interim accesses but it mandates that only the agency issuing an interim needs to recognize it. The implication is that if an agency is willing to take a risk on an individual by granting access before all clearance procedures are complete, that agency alone should bear the risk. Others are not required to join into it based on a judgment that they did not make. Over the past several years agencies have been issuing more interim clearances in an effort to have people working while they wait for their final clearance decisions. This became more apparent when a backlog of investigations built up in DoD in the late 1990s that delayed the completion of thousands of investigations, while the attacks of September 11, 2001, created an urgent demand for specialized language and analytic skills. Persons with interim clearances can rarely move reciprocally to other agencies, and typically if they do move, a new background investigation is initiated. Similarly, regulations allow agencies to grant an individual a waiver of adjudicative standards, but exceptions that make sense to one agency may not seem reasonable to another. Waivers, like interims, affect the policy of reciprocity by increasing the inconsistencies practiced across what are supposed to be uniform standards.

There are some aspects of reciprocity that currently appear not to work well. These include conversion of responsibility for accesses from one agency to another, reciprocity for industrial contractors and among Special Access Programs (SAPs), and a basic distinction among agencies between suitability and security that challenges assumptions in reciprocity policy.

The authorizing agency that grants a security clearance or access continues to exercise responsibility for its decision as long as the individual works with information in its care. For access to Sensitive Compartmented Information (SCI), only a specified group of Senior Officials of the Intelligence Community (SOICs) and their designees (defined in E.O. 12333 issued in 1981) hold the authority to grant SCI access from the Director of Central Intelligence (DCI) and,

in the executive orders ultimately by the President. Keeping track of the proper authority over a clearance when a person moves from one agency to another, the type and dates of previous background investigations he or she has undergone, and the start and end dates of a conversion challenge the existing record-keeping systems. Too many times information must be tracked down, delaying moves and adding paperwork. Differences among agencies in their procedures for initiating, tracking, and verifying conversions weaken reciprocity.

Reciprocity is one of the main goals of the National Industrial Security Program (NISP), which has oversight over personnel security for industrial contractors. The NISP includes a structure of authority divided between four co-equal Cognizant Security Agencies (CSAs), and this can challenge reciprocity. The goal of treating the many thousands of industrial contractors reciprocally with government employees runs into difficulty because it downplays an underlying difference: by definition, contractors perform specified tasks or services for a fee, while government employees are entrusted with upholding the government's interests, including its control over its sensitive information, on behalf of the nation. Contractors we interviewed noted that when contractor employees with eligibility access could not move from working on a contract sponsored by one agency to a contract sponsored by another, these failures of reciprocity continue to cost money, time, and talented potential employees who give up and move on.

Lack of reciprocity between SAPs of like protection levels was a particular problem for industry respondents, who often work for many of these programs at once. Reciprocity among SAPs is explicitly mandated in E.O. 12968, yet the several large defense industry contractors interviewed agreed that for their companies, reciprocity among collateral clearances and reciprocity among SCI accesses each worked more smoothly than it does with SAPs. SAPS seemed to respondents to resist reciprocity, and this entailed extra cost and effort for them. Numerous respondents pointed to SAPs as reluctant to recognize reciprocity, many resisting reciprocity even for visits. Despite the patient efforts by committees to identify and promote uniform procedures, respondents noted that SAP personnel understand their programs to occupy extraordinary levels of access defined in good part by themselves. Lack of trust in the judgments of others in the face of these rigorous security demands means that SAPs seem unlikely to achieve complete reciprocity.

Finally, E.O. 12968 separates determinations of eligibility for access to classified information from suitability decisions for employment or retention of employees. Decisions on suitability for hiring remain the prerogative of the agency, and reciprocity policy applies only to the decision on eligibility for access to classified information. In practice, however, the perceived security demands of various agencies blur this distinction between suitability and security. Respondents in the IC noted that the particularly sensitive work of their agencies demanded security eligibility as a condition of suitability for employment—the distinctions between suitability and security disappear when covert intelligence and analysis of SCI are the nature of the work. Whether agencies experience security and suitability as separable or inseparable divides them into two camps that are difficult to bridge with reciprocity.

Consequences of Lack of Reciprocity

Respondents agreed on the adverse impact that a lack of reciprocity has on procedures in their agencies or companies: inefficiency, waste of time, waste of money, and loss of talent when applicants cannot wait any longer for jobs or assignments. There was general agreement that improved reciprocity would increase efficiency, lower costs, and thus would benefit the government.

Reasons for Lack of Reciprocity

When asked about the reasons for lack of reciprocity, respondents pointed to two interrelated issues: turf and trust. Many pointed to a determination to exert ownership over the security clearances and accesses held within agencies that reflects the responsibility people feel for the information entrusted to their care. Having adjudicated a decision about an individual and granted access, an agency can feel that the access belongs to it. Virtually all respondents agreed that beneath the lack of complete reciprocity there is a certain lack of trust based on fear. Lack of trust is a symptom of the same structural reality that produces "turf battles." People trust what is familiar and what they can control or at least influence, and they distrust what is less familiar and what they cannot control. Investigations and adjudications done by others, even though they work with the same prescribed standards and guidelines, seem less trustworthy than those done by "our people."

Respondents pointed to various issues with both the performance of background investigations and with adjudication that they felt reduce reciprocity. These included the multiplicity of government and private entities performing background investigations that result in differing procedures and judgments. Agencies vary in the resources they can commit to personnel security: Some agencies have hundreds of thousands of investigations to process each year, others only have hundreds and can afford to perform additional procedures. Respondents pointed to the lack of uniform personnel standards for investigators and for adjudicators, and a lack of common training in both professions, as reasons for inconsistent application of guidelines. These perceived inconsistencies produced a sense that the judgment of others could be untrustworthy.

Some respondents expressed skepticism about the necessity for complete reciprocity that is mandated in E.O. 12968. The advantages of standardized and centralized personnel security procedures—benefits such as reducing costs by eliminating duplication and redundancies while increasing efficiency—can be balanced against potential disadvantages. One disadvantage mentioned is a decoupling of accountability for security from the human judgments made by an agency in its vetting procedures. Thus, reviewing the file of an existing background investigation, and possibly re-investigating and re-adjudicating, are seen as procedures that give a prudent second look by a new set of eyes—a second look that is likely to enhance the quality of the decision and therefore the level of security. To respondents who argued that complete reciprocity should not be the government's goal, the distinctiveness of agencies in the IC was more significant than the presumed benefits of standardization. These would argue that a more nuanced reciprocity, which recognized differences among the communities, should be developed.

Options for Action

1. Continue Doing More of the Same. Some respondents thought it best not to tinker further with the policies, authorities, and procedures affecting reciprocity. Among these, some felt that the current level of reciprocity was all that could be expected, while others felt that on-going work would lead to continued improvements in reciprocity.

2. Try Money. Some respondents felt that a disparity among the various agencies in the funding personnel security programs seriously hinders reciprocity, and that agencies such as DoD, the agency with a large majority of the eligibility accesses, should invest more resources in order to bring its program to a level more like those in the IC.

3. Restructure the Context for Reciprocity. Some respondents expressed frustration with the inability of "some overarching Governmental authority to impose the reciprocity standards in E.O. 12968 on the rest of the government." It has been characteristic of personnel security policy that new initiatives like reciprocity have been overlaid onto existing policies without a complete reworking and integrating of the old and the new. E.O. 12968 was a compromise in 1995 that left in place competing authorities and prerogatives. Possibly the new demands placed on the government by the terrorist attacks in 2001 have diminished the urgency of reciprocity policy for the present, but eventually a restructuring of the authorities that underlie responsibility for national security information will be necessary if reciprocity is to become more complete.

4. Eliminate the Need for Reciprocity by Consolidation. Some suggested that consolidation of personnel security functions is the best approach. Creating a single organization to do background investigations across the federal government, and a single organization to do adjudication, and a single database that would be accessible to anyone checking clearance status would simplify these functions and holds out the promise of consistency, uniformity, and accountability. However, this approach deemphasizes the distinctions among agencies, and differences that flow from them, which many find crucial.

5. Redefine Reciprocity to Reflect Differences between the IC and Other Agencies. Some argued that there are irreducible distinctions between the IC and non-IC agencies. While in this view reciprocity among IC agencies profitably could be developed further, reciprocity between the IC and non-IC agencies should be redefined to acknowledge these distinctions. From this perspective, complete reciprocity should not be the goal of the federal government and a policy with more gradations should be developed.

Table of Contents

Appendices

List of Tables

Introduction

The report that follows is an overview that evaluates the degree of reciprocity among executive branch agencies of the federal government. It traces the evolution of the three key elements in reciprocity—background investigations, adjudication, and records maintenance—from localized, distributed approaches toward greater centralization of each function. It summarizes the development of the policy of reciprocity itself. It then reports findings based on interviews with security professionals at 14 federal agencies and five contractors on the current state of reciprocity: what works quite well, what works sometimes, and what usually does not work. It reports on what the respondents perceived were the reasons for the policy's successes and failings. Lastly, it offers to policymakers possible options for action on reciprocity.

Reciprocity is a policy that requires acceptance of equivalent personnel security clearances and accesses across the executive branch of the federal government. Authority for the current reciprocity policy is found in an executive order issued in 1995 by President William J. Clinton, E.O. 12968, *Access to Classified Information*. This order mandated that "background investigations and eligibility determinations conducted under this order shall be mutually and reciprocally accepted by all," unless an agency has knowledge that the individual in question does not meet the standards for eligibility. In effect, it is this exception rather than the rule that has characterized the system. The President approved the *Adjudicative Guidelines and Investigative Standards* called for in the executive order of 1997. These were implemented in 1998 in DoD, whose employees hold the great majority of personnel security clearances, and one by one the other executive branch agencies implemented them in the late 1990s. The current policy of reciprocity has been enunciated and in effect for 6 years. It is useful to begin an evaluation of how it is working.

The term "reciprocity" implies a give-and-take relationship, or what the dictionary calls "a mutual or cooperative interchange of favors or privileges."[1] However, a mutual or cooperative interchange does not necessarily mean an equivalent or unconditional interchange. Gary Harris, Lt. Col., USAF (Ret.) has suggested that a useful way to think about personnel security reciprocity is to compare it with the issuance and use of driver's licenses.[2] His analogy illustrates some of the shadings possible in an on-going reciprocal interchange (Harris, 1998).

There can be degrees of reciprocity, or even "strings" on reciprocity that condition it. For example, in the United States, a person can pass a test and obtain a driver's license in Virginia, and then drive through the intervening states on a trip to California and continue to drive a car there. California recognizes driver's licenses issued by Virginia, and indeed this initial full reciprocal recognition of driver's licenses allows a person to drive through all of the states on a license issued by any one of them. This is so even though the tests and the requirements for getting a driver's license vary somewhat from state to state.

However, eventually this reciprocity is conditioned in specific ways. If the Virginia

---

[1] The American Heritage Dictionary of the English Language, Fourth Edition, 2000.

[2] Harris served on the staff of the Security Policy Board before moving to the staff of the Personnel Security Managers' Research Program (PSMRP). Projects, including this one, which were sponsored by PSMRP were moved under the oversight of the DCI Special Security Center (DSSC) in 2003.

tourist settles in California and becomes a resident there, in short order he or she must apply for and obtain a California driver's license. The applicant may have to repeat some of the tests that he or she just passed in Virginia in order to get a license to drive in California. So, while the mutual acceptance between state driver's licenses is full reciprocity for an interim period, once residence is transferred, reciprocity becomes partial—one may not be asked to take another road test, but may need to pass vision and driving law tests again.

Driver's license reciprocity between states is a familiar example of distinctions that are implicit in the concept of reciprocity. As Harris points out, there can be a full exchange of all privileges, or there can be a partial exchange of limited, specified privileges, and a partial exchange is still called reciprocity. As we will see, ambiguity in statements of federal policy about full and partial degrees of reciprocity has allowed, indeed has encouraged, inconsistent implementation of the policy.

Three functions comprise the personnel security system in which reciprocity is expected: performing a background investigation, making an adjudication decision (E.O. 12968 labels this an "eligibility determination"), and maintaining accurate records on the current status of an individual's accesses. In theory (or perhaps in fantasy) if one federal agency performed all background investigations using the prescribed national standards, and one federal agency evaluated those investigations employing properly trained adjudicators and making all eligibility determinations based on prescribed national standards, and one federal agency maintained a current database that could be consulted for the status on all investigations and adjudications, reciprocity between cleared personnel employed at any federal agency could be full and automatic with any other federal agency.

This is not the case in practice, for at least two reasons. First, in the past the military departments and some agencies performed these three functions (investigations, adjudications, and maintaining records of the results) for their own personnel. Only gradually over three decades has each of the functions been partially integrated in DoD and across the federal government. Born localized, none of these functions has yet matured into a full-blown consolidation, and agency-specific distinctions persist among them.

Secondly, the merging of each of the three functions is hindered because of the various distinct communities in which personnel security accesses operate. These include the community of many DoD agencies and some others that rely on collateral accesses; the community of intelligence agencies (some of which are DoD and some not) that in addition to collateral typically require access to SCI; the community of SAPs with its many industrial contractors reporting to various government agencies; and the non-DoD agencies, each with its own idiosyncrasies, such as the Departments of Energy and State and the Federal Bureau of Investigation (FBI).[3] Increasingly, as industrial contractors perform more government work, agencies in each of the government communities interact more often with industrial contractors. Some cleared people need access to information only in one of these communities, but many others move between them or need accesses sponsored by more than one of them, and this is especially true for contractors. The federal policy of reciprocity demands that distinctions

[3] Collateral refers to security clearances that provide eligibility for access to classified information at the Confidential, Secret, or Top Secret levels.

between these communities should be minimal, yet distinctions among them persist.

To sketch the background of the policy of reciprocity here, we will briefly consider milestones in the partial consolidation of each of the three functions—investigations, adjudications, and record maintenance—over the past 30 years. Only milestones that laid the basis for the policy of reciprocity are discussed here; this is not an attempt to trace the whole history of the evolution of personnel security policy. This slice of history related to reciprocity shows us repeated efforts to centralize and systematize the personnel security functions across the executive branch; these efforts have been cross-cut by resistance to change and perceived threats to agency prerogatives. Until each of the three personnel security functions was somewhat standardized, however, no one could expect reciprocity among agencies. Finally, we briefly trace the evolution of the reciprocity policy itself.

Background

Investigations

Until 1972, each of the military departments and designated federal agencies investigated the backgrounds of their own personnel. The Central Intelligence Agency (CIA), the FBI, the State Department, and the Treasury Department were among the main agencies fielding their own investigative staffs that performed background investigations on their applicants. The Office of Personnel Management (OPM) performed the background investigations of civilians for most of the other federal agencies. OPM investigated civil service applicants both to determine their suitability for federal employment under the Civil Service regulations originally dating back to 1883, and for security access, if it were needed for the particular job. The Civil Service regulations had been modified over the years, notably in 1953 by E. O. 10450, to include determining an applicant's loyalty to the nation, which initiated an overlap between suitability and security standards (Commission on Protecting and Reducing Government Secrecy, 1997).

As the Cold War deepened in the early 1950s, authorities realized that even though the world war was over, ongoing Soviet espionage demanded that classified information be safeguarded at wartime levels of security. Investigating people's backgrounds to decide whether they could be trusted with classified information, which had been a wartime practice, "settled in" as the standard practice of the federal bureaucracy (Commission on Protecting and Reducing Government Secrecy, 1997, pp. A-46-47). Given that investigations were performed by different authorities, inevitably there were some inconsistencies among investigations conducted by different agencies, and even among investigations by a single agency. Consistency across agencies was hardly to be expected as long as background investigations, even those done to determine access to classified information, remained integrated with the personnel function and were handled internally in a single agency or department (Department of Defense Personnel Security Working Group, 1974, pp. 99-100). The benefits of systematizing these procedures across the military departments and executive branch agencies, and the fairness to applicants of doing so, were argued out in studies starting in the late 1950s and continuing through the 1960s (Department of Defense Personnel Security Working Group, 1974, pp. 1-6).

The Blue Ribbon Defense Panel recommended in 1970 that DoD (the agency with the

most personnel security clearances) eliminate a costly redundancy of investigative functions and personnel by consolidating the performance of background investigations into a single Defense agency. President Richard M. Nixon responded to a request from his Secretary of Defense by combining investigations staff members from the four DoD investigative services into one agency to be called the Defense Investigative Service (DIS) (Blue Ribbon Defense Panel, 1970).[4]

DIS was established on January 1, 1972 and became operational throughout the country on October 2, 1972 (DoD Directive 5105.42, 1972). Virtually all of the new agency's personnel, resources, and facilities were appropriated on short notice from personnel security offices in the Army, Navy, and the Air Force. DIS built cohesion slowly, since personnel who had been transferred in brought with them differing procedures that took time to synthesize. After several years, the military personnel initially detailed to the new agency were replaced by civilian investigators. At its founding DIS also assumed the role of Executive Agent over the Defense Central Index of Investigations (DCII)[5] that had been started in 1967, and over the National Agency Check Center. In 1980, DIS expanded its mission beyond background investigations by assuming administration of the Defense Industrial Security Program (DISP), and by incorporating the Defense Industrial Security Institute and its security training mission. These changes enlarged DIS's responsibilities to include training security personnel and performing facility inspections for industrial contractors across the country.

The creators of DIS also hoped that the centralized investigation agency would pare down the many types of background investigations being performed in DoD. Each military service had crafted its own scope for investigations and had tailored requirements for its own needs and procedures, yet people being cleared on the basis of the differing investigations might need access to the very same classified information. As early as 1973, a DoD Personnel Security Working Group tapped members from each service to study issues that included reaching a common investigative scope, controlling the number of clearances requested, and centralizing adjudication in DoD (Personnel Security Working Group, 1974). This group's recommendations may still be appropriate for the personnel security system in 2004. Its report noted the irony of centralizing the investigation function in DIS, but leaving the authority to request investigations "highly decentralized"—at that time thousands of DoD units, offices, and agencies each could and did send requests for background investigations to DIS. This encouraged redundancy by allowing each successive agency to which a person was posted to request another investigation on him or her (Personnel Security Working Group, 1974).

DoD reached a milestone in December 1979 by issuing its first major consolidation of DoD personnel security programs in DoD Directive 5200.2-R. This regulation pulled together policies and procedures, criteria for adjudications, types and scope of investigations, due process procedures, and the assignment of program management responsibilities. It became the basic statement of the personnel security program, underwent a major revision in 1987, and is in the process of further revision in 2004 (DoD Directive 5200-2-R, 1979, pp. I-1, I-2).

---

[4] The four DoD investigation agencies that contributed to creation of the Defense Investigative Service in 1972 were the U.S. Army Intelligence Command, the U.S. Army Criminal Investigative Command, the Naval Investigative Service, and the Office of Special Investigations, Air Force.

[5] Later the index was renamed the "Defense Clearance and Investigations Index," maintaining the acronym.

Despite the best efforts of DIS investigators, by 1980 structural problems led to the first of several backlog crises in which DIS investigators fell behind and the completion times of investigations lengthened from the expected 30 to 90 days to several hundred days. DIS suffered from episodic funding problems and staff cutbacks. It also could not control its workload because of DoD's open-ended commitment to perform any and all background investigations that might be requested by several thousand authorities without mechanisms to predict, track, or control requests. In June 1981, the Deputy Secretary of Defense declared a moratorium on accepting requests for any new Periodic Reinvestigations (PRs), temporarily eliminated background investigations for Secret clearances, and revised the scope of other investigations in an effort to allow DIS to work down its backlog (General Accounting Office, 1981, p. iii). A Select Panel studied the situation in 1982 for the Deputy Under Secretary of Defense for Policy. The panel's members reported that the panel had achieved "a clear consensus of dissatisfaction with the way the Personnel Security Program now works. The primary concern expressed was with the initial investigation, its scant value and lack of quality, and the inordinate delays in awaiting the results of an increasingly shallow product" (Department of Defense, 1982. p. 1). The panel's recommendations included framing a new single-scope background investigation and a uniform polygraph policy that would apply to the National Security Agency (NSA) and the other intelligence agencies, and shifting the emphasis from initial investigation to continuing evaluation (Department of Defense, 1982, p. 2). These ideas would bear fruit in the gradual adoption of all these measures, but it would take the next 15 years.

Also at this time, reacting against the moratorium at DIS that suspended new PRs, along with the length of time DIS was taking to complete its investigations, the National Reconnaissance Office (NRO)—an agency that operates under the joint authority of the Secretary of Defense and the DCI—became the first DoD agency to decline to participate in the DoD-wide investigative services that DIS offered. Instead, NRO began to contract with a private company for its background investigations, and it has continued this approach to the present.

Later in 1981, DIS received a welcome infusion of additional personnel, over 700 people, which was meant to allow the agency to better handle its actual and anticipated workload. Except for the persistent complaint that turn-around time on results was too slow, customers of DIS background investigations during the 1980s remained reasonably satisfied with the quality of the investigations, the depth of the subject interview that was incorporated into DIS procedures, the counterintelligence analysis that was being done, the availability of polygraph testing to follow up on discrepancies, and the utility of the maintenance of records in the DCII. The rash of espionage incidents by Americans that came to light in the 1980s kept the attention of the public and the Congress fixed on the country's personnel security procedures. On January 1, 1987 the first major revision of the DoD Directive 5200.2 and its associated regulation codified many of the changes and improvements in procedures suggested by preceding studies.

An important landmark in efforts to standardize investigative policies and practices—a prerequisite for effective reciprocity—was the issuance of National Security Directive (NSD) 63 by President George H. W. Bush (Bush, 1991). NSD 63 mandated that an SSBI be adopted by all agencies and departments of the executive branch for both collateral Top Secret (TS) National Security Information, and for access to SCI. It established a minimum investigative scope and standards, but specified that investigations could be expanded "as necessary, to resolve issues

and/or address employment standards unique to individual agencies."

This represented a hard-won compromise between the collateral and intelligence communities based on empirical research that identified the investigative sources that produced the most useful information.[6] The new SSBI eliminated both the 5-year scope that was then current for initial TS clearance, and the 15-year scope for initial SCI access, which had been standard since 1953. Studies showed that so little information of adjudicative significance emerged from investigations that went back in time beyond 10 years that security could be maintained with the more cost-effective 10-year scope (Carney, 1991, p. 7). The directive also reflected the growing evidence that interviews provided considerable useful information by mandating that all SSBIs include an interview with the subject.

Since DoD continued to lack effective control over requests for investigations, it remained vulnerable to work-load problems. When staff reductions at DIS followed the abrupt end of the Cold War in 1991, while at the same time the mandate in NSD 63 that all investigations would include a subject interview increased the complexity of background investigations, completion times of investigations began to lengthen at DIS. This caused frustration among DIS's customers and, reminiscent of the impact a similar backlog had a decade earlier, when NRO turned to contract investigators, it made the goal of centralizing background investigations across DoD harder to reach. In the mid-1990s when the delays at DIS lengthened, both the NSA and the Defense Intelligence Agency (DIA) followed NRO's lead and began to outsource their investigations, with the approval of the oversight agency, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence.[7] The CIA had also been outsourcing investigations for their personnel starting in the early 1990s. In response to the lengthening completion times for background investigations at DIS, in June 1996 DoD again, as it had in the 1980s, resorted to an annual quota on the number of Secret and Top Secret PRs Defense agencies could submit to DIS. This reduced the numbers of requests for PRs sent to DIS and it allowed DIS to marginally improve its completion times on the investigations worked, but the quota led to an alarming increase in delayed reinvestigations. As the backlog in PRs snowballed and more cleared personnel continued to have access without undergoing their 5-year reinvestigation, many people thought this increased the security risk (General Accounting Office, 1999).

A major study by the Joint Security Commission in 1994 had tried to re-imagine security policies in light of the expected savings from the end of the Cold War. The Commission focused on getting the most from the money expended while getting as much security as the country could afford—hence an emphasis on risk management rather than the elimination of all risk. Among the Commission's many observations related to reciprocity was the finding that "The processes we use to clear personnel in the Defense and Intelligence Communities vary widely from agency to agency. Different standards are applied by different agencies; clearances are not

[6] The Personnel Security Working Group performed an early analysis of the productivity of sources in 1974 (Department of Defense Personnel Security Working Group, 1974, p. 100 and attachment 5); in 1990 the Defense Personnel Security Research Center did another thorough analysis for the Personnel Security Working Group. The 1990 study's recommendation was that a 10-year scope was sufficient to develop almost all issue cases, and it prevailed in the policy that was adopted in NSD 63 (Carney, 1991, p.i).

[7] The office in 2003 became part of the Under Secretary of Defense for Intelligence.

readily transferable; and the time to grant a clearance ranges from a few weeks in one agency to months in others. Accordingly, we recommend common standards for adjudications and a joint investigative service to standardize background investigations and thus take advantage of economies of scale" (Joint Security Commission, 1994, p. 4). The proposal for a joint investigative service between DoD and the DCI did not find a champion and the idea died. The Commission also suggested a "single executive committee" to create and oversee implementation of security policy, and this resulted in the creation of the Security Policy Board (SPB) by Presidential Decision Directive (PDD) 29 in 1994. The SPB met regularly from September 1994 until April 2001 when it was abolished by President Bush in National Security Presidential Directive 1 (Aftergood, 2002).

While the SPB lived during the mid-to-late 1990s, it framed and sponsored several important policy advances in personnel security. When the espionage committed by Aldrich Ames became public in February 1994 and Congress reacted with demands that personnel security be improved, the SPB coordinated the framing of a new executive order that would for the first time require financial disclosure, a measure that might have assisted in unmasking Ames sooner. The Board also coordinated policies applicable across the executive branch that implemented reciprocity in the use and inspection of facilities for classified information, reducing costly duplication of inspections and multiple facilities (Security Policy Board, n.d.).

E.O 12968, *Access to Classified Information*, issued August 2, 1995, marked the most important landmark step toward standardized background investigations by requiring the SPB to implement "a common set of investigative standards for background investigations for access to classified information." Relying on results of a follow-up study by PERSEREC in 1996 on the productivity of sources used in investigations, the President approved three federal standards that were published in March 1997 for two types of initial access and one reinvestigation for continued access (Carney, 1996; Berger, 1997). Achieving agreement on these common investigative standards, not just across DoD agencies but across all executive branch agencies, was another milestone in the effort to reach consistency. For the first time, "all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders, or grantees and their employees..." and anyone else who requires access to classified information, including collateral, SCI, and SAPs, were directed to use the same designated standards for investigations (Berger, 1997, p. 1).

The SPB contributed another significant milestone toward reciprocity with the MOA the SPB Forum researched and sponsored on consistency in polygraph policies for personnel security across federal agencies. The Forum had been established in 1994 by PDD29. It served as the working-level group that reported to the SPB. The Forum tried to consider security policy issues, develop security policy initiatives and obtain Department and agency comments on them, evaluate the effectiveness of security policies, monitor and guide the implementation of security policy to ensure coherence and consistency, and oversee the application of security policies. At a meeting of the Forum on August 27, 1998, 12 of the 13 agencies that administered polygraphs in their personnel security programs signed the MOA that had been developed, agreeing to recognize one another's polygraph results within the guidance outlined (Security Policy Board Forum, 1998).

However, at roughly the same time that these executive orders, common standards, and MOAs advanced the conditions necessary to standardize background investigations across the government, changes at DIS had the effect of undermining them. Management at DIS tried to accomplish the agency's "reinvention" ("Government reinvention" was a wide-reaching federal initiative of the early-to-mid-1990s) by unilaterally streamlining investigation requirements (Department of Defense Inspector General, 1997). A series of policy letters issued to DIS investigators starting in August 1996 strayed from the standards recently agreed to across the government. In order to save money and do more with its shrinking resources, DIS management gave its investigators broad discretion in how they would meet the common investigative standards and how they would pursue or resolve issues of security significance.

For example, DIS investigators were told they no longer needed to contact creditors about debts not listed on credit reports but that the subject later revealed during an interview. Several changes at DIS directly contradicted the new federal investigative standards, including the practice of no longer doing the mandatory local agency records checks and checks of public records on civil and criminal actions. Despite forceful objections from the SPB that these changes by DIS contravened efforts to achieve uniformity among agencies in investigative standards, DIS/DSS persisted in them until February 1999. Compounding these problems, DIS cut back on training for its investigators and eliminated two quality control mechanisms that had been designed to review investigations. It also eliminated the investigator training facility itself. Not until Congressional concern, reflected in the General Accounting Office's scathing report in October 1999, reached a high pitch did DSS change course and reverse the changes that had produced background investigations that did not reliably meet the scope of the common investigative standards (General Accounting Office, 2000).

DIS changed its name in 1997 to Defense Security Service (DSS) to reflect the greater responsibilities it assumed for counterintelligence and security education. In another reinvention move the following year, DSS implemented an ambitious automated case tracking and management system, the Case Control Management System (CCMS). Over the next several years, however, its serious inadequacies became apparent. The new system could not handle even the volume of cases that had been worked before the automation. Poor planning led to the discontinuation of the old system before the new system was proven to work—which it did not do for months (House of Representatives, 2002, pp. 29-35). During this period the backlog in investigations and reinvestigations exponentially worsened. During the backlog crisis, some of DOD's requests for background investigations were shifted to OPM while DSS sought to recover from its CCMS setback, and as an expedient, more private companies were invited to enter the field to provide background investigations. A period of bureaucratic fibrillation ensued, played out in numerous studies and investigations, about when, whether, and how DSS could recover from its backlog (House of Representatives, 2002, pp. 13-16). The combination of unilateral changes to the investigative standards that had been agreed to across agencies only a few years earlier and the backlog crisis diminished the confidence of the wider reciprocity community in DIS/DSS investigations.

Ultimately in 2003, DoD decided to procure all of its background investigations from OPM, and to transfer DSS investigative personnel to OPM as well. In effect, it gave up on its 30-year effort to achieve centralized investigation at DIS/DSS. Many of the background

investigations done under OPM direction in turn would be subcontracted to private companies.[8] DSS would keep its industrial security and security education responsibilities and a counterintelligence review function, but it would no longer do what it had originally been created to do—to conduct background investigations.

To the extent that reciprocity of eligibility determinations depends on the results of an investigation into an applicant's background that is consistent across agencies, the developments in the recent past, which eliminated DSS's role as DoD's provider of background investigations while multiplying the number and type of investigative providers among OPM and numerous private companies, kicked away one of the three pillars on which reciprocity rested.

Adjudication

The second prerequisite for reciprocity in the personnel security system is adjudication that is consistent across agencies. Adjudication is the decision-making function in which trained adjudicators consider the materials collected in a background investigation and apply the uniform federal adjudicative guidelines to an individual's application for eligibility access. Unless authorities in the various federal agencies can be assured that decisions being made in other agencies reflect common standards, they are unlikely to risk recognizing accesses granted outside their own agency.

The heads of the various federal agencies have had the explicit responsibility for maintaining programs to ensure their employees eligibility for access to classified information is "consistent with the interests of national security" since issuance in 1953 of the founding federal personnel security policy, E.O. 10450 *Security Requirements for Government Employees.* This responsibility was refined in 1981 in E.O. 12333 *United States Intelligence Activities*, which structured responsibilities within the IC for the dissemination and protection of information by the SOICs. Thus, accepting decisions made in an agency other than the one controlled by an official carries an inherent risk—a risk of relying on a judgment made in another agency about someone's trustworthiness, and being held responsible later for damage to national security should that person betray their trust. Common application of consistent standards for adjudication can in theory whittle the risk down to acceptable proportions, and so consistent adjudication is essential for reciprocity.

Consistency in adjudication implies that the application of one human being's judgment about the behavior of another human being, as that is reflected in a written report of a background investigation, will be consistent with someone else's judgment. This is a tall order. There are numerous aspects implied in achieving consistency among adjudication decisions that are made in various agencies, including everyone working with the same clear and applicable policy and standards, employing adjudicators with similar skills, providing the same training to adjudicators everywhere, locating the adjudication facility within organizations at the same level of visibility and concern to senior decision-makers, and keeping each facility above bureaucratic and political pressures (Nelson, 2003). Given the unlikelihood of reaching all these consistencies

[8]As of October 2003 this change had not yet been accomplished due to on-going negotiations about funding, control over numbers of investigations, and Congressional approval of the proposed shift of DoD background investigations to OPM.

in multiple locations, for four decades various champions—largely from DoD—have been advocating a consolidation of adjudication at as few facilities as possible.

As E.O. 10540 laid out the federal personnel security program in 1953, adjudication, like investigation, was to be localized. The executive order focused on investigation policies and standards; in passing, it did recognize that the location of the judgments to be made about an employee's reliability, trustworthiness, character, and loyalty typically would be in the personnel office of each agency. The order also blithely mandated consistency across these thousands of offices where adjudications were to be made, without considering how it might be achieved:

> WHEREAS the American tradition that all persons should receive fair, impartial, and equitable treatment at the hands of the Government requires that all persons seeking the privilege of employment or privileged to be employed in the departments and agencies of the Government be adjudged by mutually consistent and no less than minimum standards and procedures among the departments and agencies governing the employment and retention in employment of persons in the Federal service... (E.O. 10450, 1953, p. 1).

One of the first sectors to achieve consolidated adjudication was the industrial contractor community within DoD. After E.O. 10865 *Classified Information in Industry,* issued in 1960, framed a comprehensive program for industrial contractors who needed access to classified information to perform work for agencies across the government, a next step toward consolidation and consistency was the formation in 1965 of the Defense Industrial Security Clearance Office (DISCO) to process all industrial clearances within DoD, the largest of the agencies. Requests for clearances were sent to DISCO and then on to DIS for investigation. In 1980 DIS assumed control over DISCO as part of its responsibilities for the industrial security program. In the early 1980s results of investigations on contractors were sent back to DISCO for adjudication as well. After a policy shift in 1988 that was intended to keep the investigative and adjudicative functions separated, if a case were "clean," i.e., presented no derogatory information, DISCO would go ahead and issue the clearance. If, on the other hand, the case did include derogatory information, the file was sent for adjudication to the Defense Office of Hearings and Appeals (DOHA) which could provide administrative judges and personal appeals hearings.

The DoD Personnel Security Working Group (PSWG) study in 1974 had taken the possibility of centralized adjudication as its main focus. The report described collateral adjudication in the mid-1970s as a crazy quilt of local decision-making. The Air Force largely adjudicated security clearances at the base level by base commanders; the Army did adjudication at each Army installation, and in some places delegated the task further to commanders of corps or divisions. Overseas units usually did adjudication at stateside headquarters. In the Navy, commanders held adjudication authority; some consolidated it by base, others by units. Navy civilian employees' clearances were adjudicated by the Navy Office of Civilian Manpower Management. Summarizing these designations, the report estimated that there were 4,000 adjudication locations for the Navy, at least 4,000 for the Army, and 200 for the Air Force. To these were added the roughly 2,000 adjudication sites among the various Defense Agencies (Department of Defense Personnel Security Working Group, 1974, pp. 11-12). Not surprisingly, given this localized situation, there were utterly no data available on numbers of people or

numbers of files involved in adjudication, or on denial rates, costs, or anything else that would document adjudication across the programs.

On the other hand, already in 1974 determinations of SCI access across the agencies of the executive branch were comparatively centralized. Guided by the Director of Central Intelligence Directive (DCID) 1/14, SCI standards controlled the handling of information and selection of employees with access to it within the IC (Director of Central Intelligence Directive 1/14, 1994).[9] All Defense agency accesses for SCI were adjudicated by DIA. NSA had already secured the privilege of adjudicating for its own personnel. The Army and Air Force had each centralized the results of their SCI adjudications into one office, and the Navy into two offices (Department of Defense Personnel Security Working Group (PSWG), 1974, pp. 15, 64).[10]

The PSWG report laid out a range of options for consolidating adjudication, from keeping the status quo to establishing a single DoD security agency to implement personnel security in all its phases (Department of Defense Personnel Security Working Group (PSWG), 1974, pp. 152-166).[11] Several years later, in 1977, some progress could be charted when the Army and Air Force each consolidated its collateral clearance adjudication, one at the Army Central Adjudication Facility (CAF) at Ft. Meade, and the other initially in the Pentagon and later at Bolling Air Force Base. In 1979 the DoD Directive 5200.2 and its associated Regulation 5200.2-R mandated that "the head of each DoD Component, to the extent practicable, shall establish a single Central Adjudication Facility for his/her Component" (DoD Directive 5200.2-R, 1979, pp. VI-1, VI-2). Despite this policy, the Navy resisted consolidation until the espionage by John Walker, Jr. and his ring was revealed in 1985. That focused pressure on the Navy to reform its personnel security practices and led to consolidation of the Navy's collateral adjudication by 1989. Thus from thousands of sites performing adjudication in the mid-1970s, by 1989 DoD had consolidated its adjudication of collateral or SCI access into 18 facilities (Crawford, Riedel & Carney, 1991, p. 4).

In March 1991 PERSEREC began a study for the Deputy Under Secretary of Defense Security Policy (DUSP [SP]) to determine whether further consolidation of DoD adjudication facilities would "more efficiently produce the products and services provided by the current system" (Crawford, Riedel & Carney, 1991, p. iii). The study framed two options, both of which urged a further consolidation of facilities. One of the options proposed consolidating them into a single adjudicative facility. DoD decided on the more conservative approach, and implemented a version of consolidation in October 1993 that reduced the DoD adjudication facilities from 18 to 10.[12] Despite later studies that argued for the ultimate consolidation into one or at most two facilities, these 10 adjudication facilities remain in operation in DoD in 2004.[13]

The trend to consolidation of adjudication facilities was paralleled over the last three

---

[9] DCID 1/14 was renumbered DCID 6/4 on October 13, 1999.

[10] On the other hand, the actual adjudication of collateral clearances continued to be performed at various sites.

[11] This statement of the range of options the group identified continues to make suggestive reading.

[12] These facilities are: Air Force Central Adjudication Facility; Army Central Personnel Security Clearance Facility; Department of the Navy Central Adjudication Facility; National Security Agency; National Reconnaissance Office, Defense Intelligence Agency; Joint Chiefs of Staff; Washington Headquarters Services; Defense Industrial Security Clearance Office, and the Defense Office of Hearings and Appeals.

[13] Notably, the Joint Security Commission, *Redefining Security,* proposed combining all DoD facilities except NSA.

decades by a trend toward uniformity in adjudication guidelines. What in 1953 had been left to each component to implement from the general categories outlined in E.O. 10450, was regularized in 1979 in guidelines for DoD collateral security clearances that were published in the 5200.2-R. The DCI issued guidelines for SCI through repeated revisions of DCID 1/14 *Minimal Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information.* In 1981, E.O. 12333 laid out the duties and responsibilities for executing the national intelligence program and defined the SOICs, one of whom is the Secretary of Defense, who implements collateral-level clearances with one set of regulations and SCI accesses with another. Thus, for years authority for granting, denying, or revoking collateral clearances and SCI accesses flowed from two sets of issuances. The adjudication guidelines for collateral and SCI access, though similar, were still different until the issuance of E.O. 12968 in August 1995 and implemented in DoD in 1998. As discussed above, this order mandated uniform standards for both investigation and adjudication across the federal government, putting in place one uniform set of adjudicative guidelines that was a prerequisite for reciprocity.

Maintaining Records of Clearances and Accesses

The third prerequisite for reciprocity is a records system that maintains current and accurate information on the status and outcomes of investigations, clearances, accesses, and adjudication decisions for individuals across the government. Like investigations and adjudication, records maintenance has undergone a long and uneven process of consolidation and modernization since 1953.

A record of data on the date and type of background investigations had been kept in the DCII since 1967, and in the late 1970s fields were added to capture the basics of an adjudicative decision for the Army and Air Force since their facilities were centralized. This move changed the name to the Defense Clearance and Investigations Index, blessedly preserving the acronym. As of March 2000, the DCII indexed records on approximately 24 million persons (Department of Defense Inspector General, 2001). The basic personnel-based system, in which adjudicative decisions were recorded on paper forms and kept in personnel files, persisted across the military departments and Defense agencies, however, forcing security officials who needed to check on the status of a person's clearance or access from another agency to search the personnel file, and to telephone the person's previous duty station if the form were missing (Nelson, 2003). Not until the late 1990s did the efforts of various automation initiatives in DoD, the IC, OPM, and the other federal agencies come together in a series of automated databases that could be networked across systems, including the JPAS in DoD, the "Scattered Castles" system for community-wide SCI-accesses, and OPM's CVS. As millions of past and current records are being entered into these databases, they promise to capture and store complete personnel security data on individuals, and most importantly for reciprocity, to allow agencies across the government to quickly and conveniently determine the current security status of an individual by checking these databases.

Reciprocity Policy

E.O. 10450 laid down the preconditions for reciprocity in 1953 by decreeing that all government employees would be "adjudged by mutually consistent and no less than minimum standards and procedures among the departments and agencies" of the federal government. The PSWG study in 1974 noted that although DoD Directive 5210.8, which then governed civilian personnel security clearances, "encourages mutual acceptance of personnel security clearances issued by DoD Components and Departments," that directive also granted considerable latitude from its expectation of reciprocity. Clearance authorities could "review investigative files and request additional investigation, 'if deemed necessary,' even when a valid clearance exists" (Department of Defense Personnel Security Working Group (PSWG), 1974, p. 14). The authors of the PSWG study noted that many authorities "routinely avail themselves of this provision, requesting additional investigations 'to be "covered"' in the event of untoward developments." They continued, "Frequently Defense Agencies 'review' (readjudicate) personnel security files of persons for assignment to those agencies, even though the individuals concerned possess valid security clearances (Department of Defense Personnel Security Working Group (PSWG), 1974, p. 15)." In this discussion of DoD policy and practice 30 years ago, we already see two factors that in 2004 continue to prevent the achievement of reciprocity: (1) the fact that DoD policy includes a provision that allowed any agency to review files and investigate further "if deemed necessary" rather than recognize an adjudication by another agency; and (2) the practice that was already well-established in 1974 of performing another investigation in hopes of eliminating any risk that in the future a person would betray the trust granted and endanger national security.

Chapter IV of the DoD Regulation 5200.2-R in 1979 mandated reciprocity for all of DoD in clear terms: "Previously conducted investigations and previously rendered personnel security determinations shall be accepted by responsible authorities of the Military Departments, Defense Agencies, and other Components of the Department of Defense..." An investigation that had already been done by a DoD agency and that was "equivalent in scope" to the one outlined in 5200.2-R must be accepted by another agency, as long as a break in federal employment of no longer than 12 months had intervened. Adjudications and Special Access for SCI granted by designated DoD authorities "will be mutually and reciprocally accepted," again, as long as the person had not been out of federal employ longer than 12 months, "or unless derogatory information that occurred subsequent to the last prior security determination becomes known." The regulation went on to insist that an agency could not even request the investigative files for review unless "significant derogatory information, developed subsequent to the date of the last clearance or Special Access authorization, is known to the requester," or the person needs a higher level of clearance (DoD Directive 5200.2-R, 1979, p. IV-1). The exception for subsequent derogatory information has persisted in DoD policy from 1979 to the present, always begging the question of how a responsible authority was likely to become aware of such information without reviewing the person's investigative file and then performing some level of subsequent investigation.

The 1987 revision of the 5200-2-R maintained the policies on reciprocity largely intact with several notable changes. The allowable break in federal service before a person had to be reinvestigated for a security clearance or Special Access was lengthened from 12 to 24 months. In addition to new information having come to light or the request for a higher level of clearance,

agencies were also authorized to request the investigative file for review if the "most recent clearance or access authorization of the individual concerned was conditional or based on a waiver." This enlarged still further the grounds on which agencies could review and reinvestigate by claiming that a prior investigation could have identified security issues that caused the condition or waiver.

Despite the policy announced in 1987, reciprocal acceptance of prior background investigations was not automatic 2 years later, and some redundant investigations continued to be performed. Among them were several for the Comptroller of DoD, then Sean O'Keefe, who grew frustrated by repeated investigations into his background done months apart each time he moved into a different job (Nelson, 2003). O'Keefe succeeded in inserting reciprocity policy in the National Defense Authorization Act for Fiscal Year 1991. This section of the act became law in Title 10 of the U.S. Federal Code and has remained in effect to the present. It mandates that

> (a) Funds appropriated to the Department of Defense may not be used for the conduct of an investigation by the Department of Defense, or by any other Federal department or agency, for the purpose of determining whether to grant a security clearance to an individual or a facility, unless the Secretary of Defense determines both of the following:
>
> > (1) That a current, complete investigation file is not available from any other department or agency of the Federal Government with respect to that individual or facility.
> >
> > (2) That no other department or agency of the Federal Government is conducting an investigation with respect to that individual or facility that could be used as the basis for determining whether to grant the security clearance.
>
> (b) For purposes of subsection (a)(1), a current investigation is a file on an investigation that has been conducted within the past five years (Code of Federal Regulations, 2002).

National Security Directive (NSD) 63, which framed the SSBI in October 1991, likewise mandated reciprocity, which it called "transferability." The investigative scope and standards of NSD 63 were deemed equally appropriate for access to either Top Secret collateral or SCI access and, it pronounced, "No further investigation or reinvestigation prior to revalidation every five years will be undertaken unless the agency has substantial information indicating that the transferring individual may not satisfy eligibility standards for clearance or the agency head determines in writing that to accept the investigation would not be in the national security interest of the United States" (National Security Directive 63, 1991, p. 3). Again, the force of the policy on reciprocity was softened by the qualification for "substantial information" disqualifying the applicant that had arisen in the meantime.

Two of the major studies of personnel security in the 1990s, which were undertaken by the Joint Security Commission (JSC), insistently recommended that reciprocity be more fully implemented. Their first report in 1994 discussed factors that had been described to them in these terms as barriers to reciprocity:

> NSD 63 ordered that SSBIs would not be duplicated and would transfer between agencies. However, some agencies, citing variability in investigative quality, take advantage of a loophole in NSD 63 to "upscope" investigations conducted by other organizations. The variability in the quality of investigations stems from differences in use of telephone interviews (considered a substandard practice by many), number of sources contacted and number and diversity of developed leads pursued. Some agencies report results in full, detailed narratives while others use summaries. These inconsistencies serve as an obstacle to reciprocity and add to processing delays.

Nor was the JSC convinced by the arguments they heard from SAP managers, who argued that the security requirements of their particular programs demanded that they readjudicate cleared individuals for access to their programs. The Commission noted that

> This adjudication is ostensibly for "access" authorization and not for clearance, but the process is virtually the same and may be repeated over and over again depending on the number of programs involved....The Commission is not convinced that such readjudications provide additional security benefits and is concerned about the significant costs resulting from the delays such readjudications impose on the system...the validation of an existing clearance should be all that is required to give an individual access to information once it has been determined that the individual has a need to know the information (Joint Security Commission, 1994, p. 51).

As noted above, in 1995, E. O. 12968 *Access to Classified Information*, mandated that "background investigations and eligibility determinations conducted under this order shall be mutually and reciprocally accepted by all," and over the next several years agencies adjusted their agency guidance to reflect this national policy. The SPB advocated for reciprocity and its implementation, and hammered out guidelines for uniform investigations, adjudications, and facility clearances that were intended to be the working basis for reciprocity. When the Moynihan Commission's report *Secrecy* came out (Commission on the Protection and Reduction of Secrecy, 1997), it adopted reciprocity as one of the five "guiding principles" for personnel security:

> When a government employee or contractor transfers or is detailed to, or is directly hired by another agency or private contractor, that individual's clearance should be accepted by the receiving agency if it is equivalent or higher than that required for the new position and if the previous investigation and adjudication occurred within the established timeframe. Agency or program-specific supplemental forms should be eliminated (Commission on the Protection and Reduction of Secrecy, 1997, p. 81).

The second JSC report in 1999, written to evaluate progress on the recommendations of the first JSC commission 5 years earlier, optimistically declared that "With these [new uniform] standards and guidelines in place, there is no longer a legitimate reason to reinvestigate or readjudicate when a person moves from one agency's security purview to another. This policy saves time and resources and helps ensure fair and equitable treatment" (Joint Security Commission II, 1999). The commission also noted approvingly that DoD had recently issued its *Overprint to the National Industrial Security Program Operating Manual Supplement* that

replaced various SAP security manuals which had been specific to each military service with a single security manual for industry, facilitating work for multiple government sponsors. A Working Group on SAP security policies was groping toward "the elusive but desirable goal of reciprocity between the SAP and SCI communities" (Joint Security Commission II, 1991, p. 7).

Thus, during the last term of the Clinton administration, the momentum for implementing reciprocity across all the communities of the federal government was at flood tide. Impatience with the costly redundancy of duplicative personnel security procedures, which had nagged at reformers for four decades, seemed to be overcoming resistance. A warning note sounded in October 1999, however, when the DCI issued another revision of DCID 1/14, and renumbered it DCID 6/4 at the same time to conform to a new series. This 1999 issuance updated the DCID to reflect the national guidelines that had been negotiated and promulgated since 1994, but it also added an Annex F, Reciprocity of SCI Eligibility Determinations. This statement meticulously defined the exceptions to reciprocal acceptance of SCI access. It carved out the usual qualification that there must be a determination that no "substantial issue information exists since the most recent adjudication," and it reserved the right of a SOIC, or his or her designees, to "grant or deny access for reasons of operational necessity regardless of another SOIC's decision." The effect of this clarification, with its emphasis on the exceptions rather than on the achievement of reciprocity, would be to circumscribe participation of the IC in reciprocity with the wider government.

Approach

The main objective of this study was to collect information from knowledgeable individuals across the federal government that could be used to evaluate the current patterns of reciprocity between agencies for personnel security clearances and accesses. Since the policy of reciprocity applies to all executive branch agencies, a daunting number, we could not interview informants at all of them. We spoke with several key people in security and policy positions at the agencies with the largest number of clearances across the several communities. Usually we were able to speak with the chief security officer and senior staff of personnel security programs or with the directors of adjudication for the agency. We also spoke with security directors and their staff members at some of the largest industrial defense contractors. A list of the names of the agencies or companies who participated is found in Appendix A.

Semi-structured interviews were used based on a protocol developed to explore the major issues of reciprocity, distilled from experience doing personnel security research. During the interviews, informants were encouraged to expand on issues as appropriate and to apply questions to the particular circumstances and needs of their agencies. This produced narrative data that we have organized by topic in order to identify themes and majority or minority views. A copy of the interview protocol is found in Appendix B. Some of the topics included (1) what reciprocity means among the various communities, (2) whether it is possible to estimate the numbers of personnel who are affected annually by reciprocity, (3) security concerns and practices of agencies that reciprocally accept adjudications from other agencies, and (4) the impact of reciprocity for enhancing or hindering policy change.

Findings

We will discuss findings in three sections: areas in which reciprocity seems to be working reasonably well, areas in which reciprocity works sometimes and other times not, and areas in which reciprocity usually does not work. Within each section we will discuss the interplay among the different communities that are trying to maintain reciprocity among their personnel security programs.

What Works (Quite) Well

Visits. In order to perform their work, members of one federal agency frequently need to visit and confer with members of other agencies. Respondents at most agencies reported that for visits the current system for reciprocal acceptance of personnel security clearances and accesses works quite well, that is, for occasions that are bounded in time. This seemed resoundingly true for visits within DoD, and largely true for visits across different federal agencies. The two systems of certifying clearance and access between the designated security offices for collateral clearances, or the special security offices for SCI, seemed familiar and reliable to most. One person noted that even for visits, reciprocity does not prevail in every arena, and pointed to SAPs as an example. Several people mentioned that although the policy of reciprocity is widely accepted for visits, problems with the administration of visit certification can still sometimes cause glitches: occasionally paperwork can be lost or actions delayed, in which case a visitor may still be delayed or denied entrance to a facility at the gate. Since the process of visit certification is usually manual—relying on the completion of paper forms that are then sent by messages, faxes, emails, or phone calls—it is subject to time delays and administrative breakdowns.

Many respondents looked forward to the further networking of electronic clearance and access databases, which they anticipated would reduce administrative problems with visit reciprocity, so long as the databases were kept updated. By facilitating rapid and convenient checks of the type and date of a potential visitor's background investigation and the current status of the individual's clearance and accesses, accessible databases could reduce the remaining problems with reciprocity for visits.

Community Badge. Almost all respondents who commented on the IC's Community Badge thought that it has proven to be a considerable improvement to visit reciprocity and that it was working well. Dating from 1992, and participated in by 13 of the intelligence agencies in the federal government, the program offers a government or contractor badge to persons whose credentials have been vetted. It is widely accepted for visitor entrance so that a person does not have to repeatedly pass a new certification for each visit. The Badge does not, however, dispense with visitor control procedures. Typically at IC facilities, all visitors, including those with a Community Badge, pass through one controlled entrance. A person's identity and "need-to-know," required under DCID 6/4, is verified at the door. In this context, a need-to-know is the reason the visitor needs access to the facility and to specified information held within it. This is established either by checking a database for a permanent certification (a "perm cert"), or by checking with the employee to be visited and asking them to verify the person's identity and need-to-know. Even with a Community Badge, IC facilities typically require that for repeated

entry (to work on a project of some weeks or months duration, for example) a need-to-know must be established by passing certification of accesses via message, fax, phone, or email. So, while the Community Badge smoothes a visitor's entry, it does not eliminate having to certify a legitimate reason for access and then updating that certification as necessary. The Badge has been an incremental and real improvement in visit reciprocity within the IC, but it does not—and should not—eliminate identification procedures.

Updating the SF-86. As discussed above, the legal and policy authorities that define and implement reciprocity in personnel security policy include the provision that if an applicant has developed security issues since his or her most recent background investigation, another agency is justified in re-investigating and re-adjudicating. Thus, it is not surprising that in an effort to identify any security issues that have come up since the last investigation, almost all agencies require an updated SF-86 from applicants for employment. Only the Department of State (DOS) reported that as long as a person's most recent investigation was within scope and had been favorable, they did not routinely require an updated form each time a person with a previous clearance applied to them for employment. Most agencies had a blanket policy to require an update, but some variations exist: NRO, for example, reported that typically they would not require the update if an individual had filled out the SF-86 within the previous 6 months. Several industry respondents noted that their sponsors found it acceptable for a person to update the form in pen and ink on the last version and sign the changes.

In 2003, the OPM released an electronic form, the SF-86C, which may be filled out annually to update clearances (Gruber, 2003). The SF-86C was a project sponsored first by the SPB and then advanced by the Bush administration's E-Government initiative. As it comes into wider use, this form promises to simplify the updating of personal information because instead of starting over each time, a person can enter any changes that have occurred over the year on the previous year's form, and save it for the next update. Since it is electronic, the update will be accessible in automated databases, which should make it easier to verify the current status of a clearance, thereby contributing to reciprocity.

Respondents assumed that asking applicants with previous clearances to update the SF-86 was sensible, since it takes advantage of the most readily available means—asking the subject—to collect recent data about the period since the person's last investigation. An applicant's behavior and circumstances since his or her last investigation were obviously not subject to adjudication by the sponsor of the prior clearance, so requesting the information and making a judgment about it—in effect, re-adjudicating—seemed to our informants not redundant, merely prudent. Even on this point, however, where there was widespread agreement that updating the form is efficient data collection, that it should be done, and that it does not violate reciprocity policy, the procedures for updating were not wholly consistent across federal agencies. The inconsistency multiplied the effort it took applicants and their security offices to comply.

What Sometimes Works

A second set of findings describe aspects of areas that seemed to achieve reciprocity some of the time but not others, or that were in the process of undergoing improvements that promised to solve many of the current problems.

Electronic Databases. During the past 5 years, the federal government has put great and accelerating effort into standardizing electronic storage of data to allow its use across multiple agencies. The current resources and initiatives to update, expand, and network together electronic databases that are most likely to affect reciprocity include the following:

- Clearance Verification System (CVS) [OPM's e-Government Initiative]
- Joint Personnel Adjudication System (JPAS) [DoD]
- Scattered Castles [CIA and the IC]
- Defense Clearance and Investigative Index (DCII) [DoD]
- Central Personnel Clearance Index (CPCI) [DOE]

Respondents strongly agreed that reciprocity depends on access to up-to-date, accurate information about the current status of clearances and accesses, the type and date of background investigations, and an explanation of exceptions, issues, and adjudicative reasoning. They also agreed that this ideal does not yet exist, but that progress was being made toward it.

Since over three fourths of clearance-holders are sponsored in DoD agencies and departments, not surprisingly the DCII was cited as the electronic database most often consulted. Other agencies and communities, such as the Department of Energy (DOE) or the IC, rely on their own specialized databases for employees and others with access to Restricted Data or SCI. The CIA has developed a classified database for SCI accesses called Scattered Castles that is coming into use across the IC. The networking being done to link or exchange some types of records between these various databases was eagerly awaited by most respondents. Many informants expected that DoD's JPAS, which will document adjudication decisions in DoD, would facilitate reciprocity by offering timely and convenient data to agencies across the government that were checking on a person's clearance status. With the data links between JPAS and OPM's CVS recently in place, this linkage further enhances the ability to quickly check a person's status. Other respondents were eager to see the DoD's Automated Continuing Evaluation System (ACES) program in action, since its automated data-mining routines promise to enhance considerably the continuing assessment of cleared personnel now done with reinvestigations.

While there was much enthusiasm among the informants for these automated tools when they are eventually up and working, and working smoothly, there were complaints and cautionary notes as well. One respondent noted that the DCII masks certain fields, such as open criminal investigations, from the view of those consulting it (although these fields are not masked from adjudicators at the CAFs). Understandably, the criminal investigative community vetoed sharing information on open criminal cases to any DCII users except the CAFs, although knowing that such an action is pending would be very relevant to an agency that is considering the person for access or employment in a sensitive position.

Another user noted that they could not rely solely on records in the DCII, because experience showed that the database did not reveal all the relevant issues and the rationale that adjudicators at the CAFs had considered. Several other respondents noted that any database needed to include text from the reports on the investigation and adjudication that described issues

and reasons for decisions, not just coded responses. The intention in JPAS to show issues that were addressed in an adjudication decision, but not the reasoning behind granting a clearance despite those issues, was cited as a problem, since for someone checking the database it raised concern without providing the means to allay that concern. One informant insisted that to be useful, updates to the JPAS database must be done daily, if not hourly. Another cautioned that relying on data mining with ACES would demand very different training for adjudicators used to the current story-based method, and that this expansion of training to rely more on data mining could prove costly.

Review of the Files of Prior Background Investigations. Asked whether their agencies typically request the investigative file of previous background investigations when a person with clearance applies for employment, five out of eight respondents to this question said that they did so routinely, while three said they did so rarely. The reasons given for why files were requested and reviewed clustered around several related concerns. Interviewees typically assumed that the particular demands of their own agency required extra caution. Some felt that because these demands were above and beyond the norm, prudence dictated a review of the investigative file in order to meet their agency's security responsibilities. Others felt that the background investigation gave information that was necessary for screening personnel for suitability. Notes paraphrasing interviewees' views capture the flavor of their concerns. The respondent from the Office of the Joint Chiefs of Staff (OJCS) pointed out that "the extreme sensitivity and high visibility of assignments to the OJCS" required the routine procurement of all investigative files for suitability decisions and for potential security issues. Department of Justice (DOJ) respondents admitted there was little or no reciprocity for clearance or access on persons seeking employment who come with clearance from another agency: typically the applicant to DOJ would receive an interim clearance while he or she updated the SF-86, and the security office reviewed the investigative file and did a re-adjudication, sent new fingerprints to the FBI for a criminal history check, and ran a credit check.

The CIA respondents explained that the agency's reliance on SCI required them to "call up the file," and to review and update it, using investigators working under the agency's direction. Respondents from DOE noted that after verifying an applicant's identity and previous access and reciprocally granting DOE access, DOE routinely obtains the prior investigative file for review. This is to ensure that the prior investigation meets national standards and that no relevant issues were unresolved that might bring into question the person's eligibility to hold a Q access. DOS respondents said that "even with a timely, accurate, and secure government-wide clearance database, DOS would still require the procurement of all prior files in order to ensure that there is nothing in the person's background that could make them unsuitable for the foreign service, especially assignment overseas." With the unique requirements of each agency's work in the forefront of their attention, these requirements outweighed the advantages to the system (cost, efficiency, or avoiding redundancy) of reciprocally accepting clearances that met scope and national standards.

The phrase "that met scope and national standards" itself can be the reason that agencies call up the files of past investigations. Over the past 10 years, the number of agencies and private companies doing background investigations has multiplied. Despite the fact that E.O. 12968 puts everyone working under common investigative standards for collateral clearances and special

accesses, there are perceived differences among these investigations in method, quality, and assiduousness. Procedures that seem to one agency to be meeting national standards do not seem so to another, as will be discussed in more detail below in the finding on investigations themselves. Because there are differences of interpretation that are reflected in differing procedures, and because there is a consequent hesitancy to rely on the judgments of others rather than on one's own best judgment, exercising due diligence is seen to require reviewing the prior investigative file.

Of the three agencies that reported they did not routinely review investigative files before granting clearance or access, the respondents from Department of the Treasury said that if an issue surfaced on the updated SF-86, then they would be likely to request the past file, and that they would also make such a request for particularly sensitive positions. NSA and DIA both noted that they did not routinely request the investigative files on personnel coming from other agencies as long as the SSBI had been within scope and done in the last 5 years; however, because their work routinely involves SCI their security screening procedures include one of several types of polygraph tests. The degree of reciprocity on polygraph testing is a separate factor, discussed below, but since polygraph testing offers another avenue for collecting data on applicants, it can serve as a substitute for or adjunct to a review of the file of prior investigations.

On the question of whether reviewing the prior investigative file constitutes a "re-adjudication," responses were mixed. Those agencies in which a trained adjudicator routinely reviewed the past investigative files saw this as a small-scale re-adjudication; those in which other security staffers looked at the files rejected the characterization of this step as a re-adjudication. There was general awareness that policy and regulations do not allow re-adjudication of a past investigation without good reason, that is, without new security issues having arisen since the last adjudication. For many respondents, the need to check for new issues since the last investigation, however, justified reviewing the past investigative files.

Respondents recognized that efficiency is forfeited when a person with a clearance or access at one agency cannot start work at another without a review of his or her prior investigative file. Some DoD staff members estimated that obtaining an actual paper file from the DSS took 30 days, and since records before 1998 had been distributed on microfiche, the older records arrived in a technology that is no longer user-friendly. More recently DSS scans files of past investigations into electronic format so they can be transmitted more conveniently. Respondents at the DOJ estimated that procuring a prior investigative file, evaluating an updated SF-86, and submitting a new fingerprint card to the FBI might take weeks before a new hire, already cleared in previous employment, could start work. DOS estimated it took 30 to 60 days to retrieve a prior investigative file. One defense contractor reported that a "cross-over" move, in which, for example, someone with a collateral clearance adds SCI access, now took 2 to 3 weeks from CIA. Industrial contractors reported widely varying waiting periods while investigative files were checked by a different agency from the one sponsoring an access, from several days to several weeks to several months.

Polygraph Reciprocity. There are differences of opinion about the reliability of polygraph testing. These differences are based on judgments about the scientific reliability of the procedure, the fact that polygraph results are not admissible as evidence in legal proceedings,

and the impact of the polygraph on privacy and employee morale (National Science Academy, 2002). Agencies in the IC typically rely on the technique and use it routinely for suitability determinations as well as for counterintelligence screening. Others, including the military departments of DoD and, until recently the FBI, exempt most of their personnel from having to undergo it, although they do maintain active polygraph programs. Given such distinctions, it is not feasible to require reciprocity across all federal agencies on the issue of polygraph testing. Instead, those agencies that do incorporate the polygraph into their security procedures work reciprocally with one another based on a MOA reached in 1998 under the auspices of the SPB.

Information from respondents suggested that IC agencies were often willing to accept a favorable polygraph from another IC agency—and not to insist that the applicant take another test—depending on which agency performed the test, and for varying lengths of time before they demand a test of their own. IC agencies make distinctions between types of polygraph tests. Two basic types are the Counterintelligence (CI) scope and Full-scope (the latter a more extensive probe of personal circumstances and behavior than the CI). Rules for when polygraph testing is required also vary at IC agencies by the type of access contemplated. For example, CIA requires all new hires or persons who will have "staff-like access" (persons who are not hired as employees of the agency but who need access to SCI to perform specific work) to undergo a Full-scope polygraph. If a prospective employee comes to CIA with a favorable Full-scope polygraph from another agency done within the last 3 years, however, respondents noted that another would probably not be required. No matter how recent, a CI polygraph given at another agency would not be acceptable for employment at CIA, and the agency would administer a Full-scope polygraph to such applicants.

NSA allows a person with a previous favorable CI polygraph from another agency access for 90 days. For longer access, however, the person must undergo and pass a Full-scope polygraph within the first 6 months at NSA. If the person is coming from CIA to NSA and has had a favorable Full-scope polygraph test in the last 5 years, however, NSA will accept that. NRO, whose personnel are largely detailed from other IC agencies or military departments, accepts a favorable CI polygraph from other IC agencies if performed within the previous 5 years. CIA and NSA both have requirements for random polygraph testing of employees within specified lengths of time, e.g., a test sometime between 3 and 7 years.

Respondents at each of these IC agencies characterized the polygraph policies and procedures at their agency as clear and reasonable, designed to fulfill that agency's responsibilities for protecting national security information with the most effective tools available. The imposition of repeated polygraph testing on persons moving between IC agencies for short-term work or for employment was seen as a cost to be borne by the individuals, and by the federal government, for security. Respondents among industrial contractors who worked on SAPs found the distinctions on polygraph testing made by the various agencies especially onerous to track and challenging to have personnel at hand who have the necessary and current tests for the available work.

Expedients Adopted to Make Things Work That Affect Reciprocity

Various measures have been adopted to move people more quickly through personnel security procedures into their jobs. These expedients do have the effect of smoothing the path through what can sometimes be a bureaucratic thicket, but they also have impacts on the policy of reciprocity because they are not practiced consistently or even recognized across agencies. Among these measures are the granting of interim clearances and waivers.

Interim Clearances. Granting an interim clearance means putting a person to work with access to classified information before all the prescribed steps of background investigation and adjudication have been completed; once all steps are completed, the interim clearance is converted into a full clearance by the appropriate authority. The DoD Regulation 5200.2-R defines as interim clearance as "A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements" (DoD Regulation 5200.2-R, 1987, p. 9).

E.O. 12968 specifies that interim clearances, which are termed "temporary eligibility" in the order, only apply at the agency that issues them; they do not have to be reciprocally honored by other agencies. The implication is that if an agency is willing to take a risk on an individual by granting access before all clearance procedures are complete, that agency alone should bear the risk and others are not required to join into it based on a judgment that they did not make. Since the backlog crisis developed at DSS in the late 1990s, delaying the completion of thousands of investigations, agencies have turned to issuing more interim clearances in an effort to put people to work while waiting for the final clearance decision.

Respondents at some agencies thought interim clearances should be issued regularly when a person comes to an agency having already been cleared by another federal agency. DOJ officials considered it a problem for reciprocity that there is persistent unwillingness to issue interims while waiting to review an investigative file or to check fingerprints on a person whose investigation was current and within scope. If a person were trustworthy days earlier at DoD, for example, the risk seemed to them small to put him or her to work at DOJ while these processing steps proceeded. Costly delays would be avoided if interim clearances were consistently administered so that a person could go to work while his or her security clearance was being finalized. DOJ typically would issue interim clearance to someone coming in with a current DoD clearance while they requested the investigative file. Similarly at the Department of the Treasury, respondents explained that if a previously cleared person comes to Treasury, even if their background investigation is beyond the 5-year mark, they would receive an interim clearance while Treasury initiated an updating investigation based on a new SF-86.

At the OJCS, the security officials grant interim TS-SCI clearance to military personnel who come with an investigation that is within scope, but they hold a pre-screening interview, require an updated SF-86, and request the investigative file for review in the meantime. For civilians and contractors, SCI access is approved at DIA. The OJCS rarely grants interims to civilians, and it does not accept interim clearances that have been issued by DISCO to contractors.

NSA's policy is not to accept interim clearances granted by other agencies. Yet it finds that circumstances since the terrorist attacks of September 11, 2001, with increased demand for linguists and other specialized personnel, necessitate exceptions. For example, military personnel assigned to NSA with an interim SCI access from their service CAF can find their final clearance delayed for months because of the time it takes to complete background investigations. NSA allows such individuals to work at the agency but specifies various conditions: the NACLC/Credit portion of their SSBI must be favorably completed; they must pass a CI-scope polygraph test; they will not be given access to the NSA information technology network with interim access; and they will be issued a special badge noting their interim access.

DIA also finds itself forced to issue interim SCI accesses despite its reluctance to do so. The agency issues an interim access to persons whose SSBI is outdated if their break in service is not longer than 24 months, a review of prior investigative files is favorable and included no waivers, and if no issues appear on an updated SF-86. At the same time, DIA initiates a new SSBI concurrent with the interim access. Respondents at DIA noted that the recent lengthy completion times for SSBIs forced them to issue interim accesses lest key personnel such as military attaches should serve their whole year or 2-year assignments overseas and return before the investigation was finished. The agency estimated that around 2 % of the SCI accesses they issue are interims.

Industry respondents also described frustration with delays of investigations and the inconsistent acceptance or rejection of interim clearances or accesses as a work-around. Security officials at one large industrial contractor speculated that to move more quickly, the personnel security system could begin issuing interim Secret clearances, but they predicted these would not be accepted in caveated or SAP programs that refuse interims per se, and that interim Secret clearances would cause problems with Foreign Government Information (FGI). For example, how would a person issuing an interim clearance in one agency know the standards that had been agreed between DoD and a specific foreign government?

Waivers. It is possible in the personnel security system to grant an exception to the standards. In DoD, 5200.2-R defines a waiver as

> Access eligibility granted or continued despite the presence of substantial issue information that would normally preclude access. Agency heads or their designees approve waivers only when the benefit of access clearly outweighs any security concern raised by the shortcoming. A waiver may require special limitations on access, additional security monitoring, and other restrictions on the person's handling of classified information beyond normal need-to-know (DoD 5200.2-R, 1987, p. 9).

Agencies and departments vary in their willingness to grant waivers. Like interims, waivers are another type of expedient that allow utilization of an individual who would otherwise be waiting for security processing, but with waivers the issue is not timeliness but an issue in his or her record. Also like interims, waivers have an impact on the policy of reciprocity by increasing the inconsistency in the system. An adjudicative decision to make an exception on an issue that is based on the experience, reasoning, and culture at one agency may not make sense or fit into the experience, reasoning, and culture at another agency. This discomfort lies behind

the demand that electronic databases such as JPAS and CVS report not just the fact of a waiver, but the reasoning and mitigations behind the grant of a waiver so another agency's officials can follow the reasoning for themselves. Waivers typically attract increased scrutiny from agencies considering an individual for reciprocal clearance or access, and they may prompt refusal. NSA, for example, finds that the military personnel assigned to the agency come with more waivers by military CAFs than NSA itself would grant. NSA adjudicators reviewing files on military assignees have found exceptions that seem jarring, such as a person whose father and uncle are in prison in Iran for spying for the KGB, and no reasoning or mitigation is stated for the grant of access. If the adjudicative outcome does not include the context and reason for the decision, it is difficult for another agency to place trust in and accept a judgment made elsewhere that could put their information at risk.

What Works Imperfectly

Some aspects of the personnel security system are not working very well to achieve reciprocity. These were the persistent sticking points that respondents identified as among the processes and issues that block reciprocal acceptance of clearances and accesses.

Conversions. The agency that grants a security clearance or access continues to exercise responsibility for its decision as long as the individual works with information in its care. Only a specified group of SOICs and their designees, as defined in E.O. 12333 in 1981, hold the authority granted them by the DCI and, in the executive orders ultimately by the President, to grant access to SCI. When a cleared individual with access from one agency, such as the Department of the Army, retires and goes to work for another agency such as NSA, and thereby also moves from the purview of one SOIC to that of another, his or her SCI access typically would be converted from the Army to NSA. If the member of the Army is visiting or just working temporarily at NSA, however, the Army continues to "own" that access determination. Keeping track of the proper authority over an access eligibility when a person moves from one agency to another, the type and dates of previous background investigations, and the end and start dates of a conversion itself, are challenges not always met by the existing or legacy record-keeping systems currently in place.

Among the many Defense agencies, for example, a clearance issued by the Army CAF that needs to be converted—also known as "recertified"—to the Defense Logistics Agency is handled by sending a request to the Washington Headquarters Service (WHS) CAF to be changed in JPAS from the sponsorship of one DoD agency to another. This changes the date of the clearance and it documents when the new sponsorship begins, although the date of the background investigation remains unchanged and that date continues as the basis for determining when within a specified number of years the next PR should occur. On the other hand, neither the Department of the Treasury nor the DOS finds it necessary to convert a valid active clearance from another federal agency when an individual enters its employ. Instead, both review existing investigative files and update the SF-86 or ask for a new version, and then import the date of the prior clearance into their oversight with its original date of granting along with the 5-year reinvestigation date based on when the investigation was completed. Respondents at DOE reported that occasional exceptions may be considered at DOE if an individual from another agency whose prior clearance is outdated is urgently needed. These are examples of differences

in the treatment of "handing off" authority over a clearance or access from one SOIC to another, or even within the many agencies of the DoD SOIC, that makes conversion an issue for reciprocity.

Reciprocity for Industrial Contractors. In 1961, with Cold War tensions apparently likely to persist indefinitely into the future, Dwight D. Eisenhower noted in his last speech as President the unprecedented growth of a "military-industrial complex" in the United States as a result of the contest with the Soviet Union (Eisenhower, 1961). There had not been a need for a permanent armaments industry until the Cold War made it necessary. Over the subsequent five decades, there has been a steady expansion of the interrelationships between private industry and the military and defense agencies. Since the fall of the Soviet Union in 1991, public policy tried to shrink the federal government to capitalize on a "peace dividend," but there has been a countervailing expansion of contracting with private companies through "outsourcing," which has made private contracting ever more important (Peckenpaugh, 2003).

Since DoD did the lion's share of contracting with industry, early in the Cold War period that agency took the lead in regularizing security policies for its industrial partners which required access to classified information to perform their work. E.O. 10865 *Safeguarding Classified Information within Industry*, was issued in 1960, the DISP began in 1976 and was reframed in December 1980 in DoD Directive 5220.22, *DoD Industrial Security Program*. This directive structured authority over security procedures to be followed by industrial facilities and industrial personnel working in all DoD components and, through agreements with the heads of other executive branch agencies, by other "user agencies" that sought to participate in the DISP. In the 1980 Directive, DIS was made the administrator of the DISP with "security cognizance for all contractors and industrial facilities..." (DoD Directive 5220.22, 1980, p. 2). Two DoD publications to guide the program were also authorized: one outlining the policies and procedures for government agencies, the *Industrial Security Regulation* (DoD 5220.22-R) and the other outlining requirements and procedures for government contractors, the *Industrial Security Manual* (DoD 5220.22-M). DIS administered the DISP through a staff of Industrial Security Representatives that inspected industrial facilities and, if they were adequate to store classified information, issued facility clearances. DIS also provided advice and security education to the security staff member on site, the Facility Security Officer (FSO). Reception of requests for clearances, adjudication of cases without issues, and records maintenance of industrial clearances was, and is, done at DISCO, the agency devoted to industrial security clearances since 1965. Thus DoD developed several decades of experience as the lead agency overseeing industrial security for itself and for most of the other federal agencies.

Momentum to further standardize the industrial security program built up in the late 1980s as part of the demand to reform the personnel security program that came from groups such as the Harper Committee, which focused on problems with industrial security after the James Harper espionage case (Department of Defense Industrial Security Review Committee, 1984).[14] The larger industrial contractors encouraged reform, citing their need to juggle too many different standards and procedures for various agencies which resulted in increased cost and delays. As a result, in January 1993, E.O. 12829 established the National Industrial Security

[14] James Harper used the access of Ruby Schuler, a secretary to an official of an industrial contractor, to sell classified documents.

Program (NISP). Built on the earlier DISP, the NISP now became a program with national scope, applicable to all executive branch agencies. Instead of authority being focused in one agency, the DoD, and extended through voluntary agreements with other user agencies, the NISP recognized four CSAs, the DoD, CIA, DOE, and the Nuclear Regulatory Commission (NRC), with co-equal authority for the program. Policy oversight of the program was lodged with the Information Security Oversight Office (ISOO), a non-DoD agency, on behalf of the National Security Council. DoD retained operational oversight as the designated Executive Agent with responsibility for issuing the operating manual, the NISPOM. DIS (now DSS) continued as administrator of the NISP, doing facility inspections, monitoring, and security education. A NISP Policy Advisory Committee (NISPPAC) was set up to regularly bring together representatives from the various government agencies and industry to discuss the program and make recommendations for change (E.O. 12829, 1993).

Reciprocity was one of the main goals enunciated in E.O. 12829, and it is for this reason that a brief background on the evolution of the NISP is germane to this study of reciprocity. The executive order called for a "single, integrated, cohesive system for safeguarding classified information held by industry" to be accomplished through four goals: achieving uniformity in security procedures; implementing the reciprocity principle in security procedures, particularly with regard to facility and personnel clearances; eliminating duplicative or unnecessary requirements, particularly agency inspections; and achieving reductions in security costs.[15]

Thus when we asked participants in this study about practices and issues in reciprocity related to industrial security, we asked about only one of the closely interrelated goals of the NISP. It is difficult to have reciprocity unless there is basic uniformity among the units that interact, and eliminating duplication is also likely to reduce costs, so these goals support one another. Not surprisingly, respondents found it difficult to talk only about reciprocity and not about related issues in the NISP program and goals.

The NISP aims to treat security for industrial contractors with the same standards and with most of the same procedures as those for military and civilian employees of the federal government. DOJ officials echoed these goals, noting that "there should be no difference between government and contractor personnel as far as reciprocity of clearance and access is concerned." Most respondents did not think things worked out this way in practice. One contractor informant expressed frustration with being a "second-class citizen" who was assumed by government employees to be working for self-interest rather than for the government's best interests. The drive to increase "outsourcing" of government work to private companies seemed to this individual to be contradicted by the pervasive distrust, and even contempt, held for contractors.

Some of this attitude is probably the result of procedures designed to ensure the

---

[15] These four goals are described as the four "tenets" of the NISP consistent with E.O. 12829 in an informational brochure by the Information Security Oversight Office titled "The National Industrial Security Program," available at the ISOO website: isoo@nara.gov. These four "tenets" are not found in E.O. 12829, although aspects of them such as consistency are implied. They are more clearly stated, though with somewhat different wording, in DoD Directive 5220.22-M, the *National Industrial Security Program Operating Manual*, January 1995, sections 1-102 and 1-207.

government's control over the classified information entrusted to contractors, and the larger issues of protecting the government's interests and maintaining fairness among various competing contractors. A contractor's request for a visit or a meeting that would involve classified information with personnel at another agency or another contractor, for example, must be approved by their Contract Office, and many respondents noted the considerable bureaucratic overhead required to "get a note" each time they needed to interact with someone else. The system assumes that since it is the government's information, the government controls when and to whom that information can be disclosed to another contractor or agency. By definition, contractors provide support and services to the government for a specified fee, and as a consequence, they are subject to management designed to protect the government's interests. The goal of treating contractors and government personnel reciprocally and essentially the same in security matters does gloss over an underlying difference between them.

Various problems that diminished reciprocity between contractors who work for more than one government agency were noted by respondents. One pointed to the lengthy delays in completing background investigations that have persisted since the late 1990s which, in his view, fell especially hard on contractors trying to move between projects to take advantage of time-perishable opportunities. Others described government agencies that still require their own paperwork forms, which insist on their own security inspections of the contractor facilities rather than relying on a single inspection, or which circumscribe access by contractors to electronic databases needed to check an applicant's current clearance or access. One large industrial contractor suggested that "interrupted Periodic Reinvestigations" were a real inefficiency for his company. These develop when a PR is started on a cleared contractor employee working on one government contract, but the person then moves to work on a contract for another agency or, in particular, on contracts between SAPs. With the employee working under different sponsorship, the initial PR is discontinued and a new one subsequently initiated, losing time and effort.

Respondents agreed that the variety and complexity of security requirements among SAPs continue to bedevil contractors, while granting that this issue has been discussed for a decade and is the subject of on-going committee work to carve out areas of consensus. Industry respondents wished for more uniformity in the application of SAP security standards than currently exists. One individual noted that the only way efficiently to thread through the current SAP system was by cultivating good personal relationships with the security managers one dealt with in order to massage out inevitable kinks with phone calls and personal entreaties.

Other issues that reduced reciprocity for contractors centered on differences between DoD and DOE. One respondent found inconsistent standards relating to "Foreign Ownership, Control, or Influence" (FOCI) between the two agencies, and with international and multi-nation contracts becoming more common, this inconsistency was troublesome. For example, should a company expect a facility clearance for a subcontractor whose president is a naturalized American citizen but whose directors all live in Sweden while they manage the company from there? In their experience, respondents found decisions on such points by DoD and DOE to differ. Similarly, respondents reported that with a DOE collateral clearance, one was likely to move smoothly to DoD, but that movement from DoD to DOE would be more often held up. The experience was that DOE was less likely to honor a DoD clearance without additional processing.

Other sticking points for reciprocity included accreditation standards for computer systems that are used for classified information. Recently revised, Chapter 8 of the NISPOM on Automated Information Systems specifies a particular technical standard for computer systems on DoD installations, while for SCI, Sensitive Compartmented Information Facilities (SCIFs) follow different standards as outlined in DCID 6/9 and in DCID 6/3 *Protecting Sensitive Compartmented Information within Information Systems*. The growing designation of Sensitive but Unclassified Information (SBU) also frustrated contractors because although they were mandated to protect this class of information, they reported little agreement between agencies on a definition for it. One respondent claimed there were 85 different terms used across federal agencies to define SBU information, a situation that required contractors to track and shape their procedures to many of these varying conceptions.

The NISP mandates the authority of four federal entities as co-equal in cooperation in industrial security: the DCI over SCI, the Secretary of Energy and the head of the NRC over Restricted Data and Formerly Restricted Data, which involve nuclear information, and the Secretary of Defense over national security information. Since the NISP is patterned after the earlier DISP and it designates the DoD as Executive Agent for the program, in effect it recognizes DoD's long experience with a functioning industrial security program as well as that agency's preponderance of the industrial security clearances. However, each of the co-equal partners aggressively guards the authority it holds over its own unique types of information, and this can cause multiple inspections, varying standards, or redundant paperwork in spite of the stated goal of reciprocity. More than half the industrial respondents drew attention to the disbanding of the SPB in 2001 as a loss for reciprocity in industry, since they felt the SPB had served as a rare forum in which to discuss issues and coordinate work on solutions.

Special Access Programs. This study could not delve very deeply into the operations of SAPs, but respondents did report a cluster of on-going reciprocity issues relating to these programs. SAP reciprocity, that is, lack of reciprocity between SAPs of like protection levels, was a particular problem for industry respondents, who often worked for many of these programs at once. Reciprocity among SAPs is explicitly mandated in E.O. 12968: "Except where there is substantial information indicating that the employee may not satisfy the standards in section 3.1 of this order, an employee with existing access to a special access program shall not be denied eligibility for access to another special access program at the same sensitivity level as determined personally by the agency head or deputy agency head, or have an existing access eligibility readjudicated, so long as the employee has a need for access to the information involved" (E.O. 12968, 1995, sec 2.4.b).

Among respondents in this study, several large defense industry contractors agreed that for their companies, reciprocity among collateral clearances and reciprocity among SCI accesses each worked reasonably smoothly, but that SAPs resisted reciprocity and that this entailed extra cost and effort for them.

By definition, a SAP is special in its security requirements. To protect the extremely sensitive information in and about their work, SAP program managers may insist on additional security procedures. An example of such a procedure is the requirement typical among SAPs that

an applicant update the SF-86 not annually, but 90 days after the last investigation if he or she is seeking access in a different SAP. Efforts to standardize security measures among SAPs have been underway for at least a decade, with some significant results. In 1994 the Office of the Secretary of Defense (OSD) strengthened management over SAPs by creating an oversight committee and a working-level committee charged with annually reviewing and validating all programs. "The [annual] review also provides an avenue to ensure reciprocity and eliminates redundancy in similar programs," a descriptive bulletin noted at the time (Deputy Secretary of Defense, 1994). In February 1995, DoD published the initial version of the National Industrial Security Program Operating Manual Supplement, the NISPOMSUP. The NISP Operating Manual would serve as a baseline standard of security procedures for collateral level industrial security, and the Supplement outlined enhanced security procedures for SAPs and SAP-type compartments, SCI and DCI-SAP-type compartments, Critical Restricted Data (nuclear-related materials) at Secret and Top Secret levels, and specified types of SAPs (DoD 5220.22-M-Sup 1, 1995, foreword). The Supplement is an acknowledgment of the four separate authorities that are trying to cooperate in the NISP (DoD, DOE, NRC, and CIA), and that each authority retains control and responsibility over information in its designated realm.

A further step toward standardizing SAP security policy within DoD was taken in January 1998 with the publication of the DoD "Overprint" to the NISPOM Supplement. The Overprint published in a single document the security requirements applicable to three different protection levels of SAPs across DoD. Its goal was to facilitate reciprocity, clarify requirements, and promote uniform implementation of the standards (DoD Overprint, 1998). The Overprint was the accomplishment of several years of meetings and work by representatives from industry, the SAP Security Standards Working Group (a result of a Moynihan Commission recommendation), and the Military Services. The complexity of defining common ground among SAP-type programs that defy commonality, however, is illustrated by the following statement in the foreword to the Overprint: "General reciprocity applies if a SAP operates at the full levels of protection of the Overprint. Specific reciprocity allows specifically identified areas of reciprocity for those programs which operate with waivers, or programs which have exercised 'commensurate protective measures.' Specific reciprocity requires mutual agreement." At a minimum, the Overprint summarized the DoD-wide expected SAP security measures for industrial contractors who were juggling multiple contracts.

Some respondents described expedients that contribute to a workable level of reciprocity among SAPs in DoD and between DoD and some other agencies. For example, a tier arrangement among SAPs operates apparently without DoD sanction, although the Air Force has formally implemented it. In the first tier, the contractor's security officials first evaluate the individual's application, which would include the updated SF-86 and supporting materials, and if it looks promising they send the packet on to the Program Security Officer for the particular SAP. This Officer adjudicates the application and returns a decision on it. In the second tier of review, an applicant submits a full Program Access Request (PAR) for SAP access, and the contractor's FSO checks off on a cover sheet whether first, second, or third tier processing is suggested for the attention of the Program Security Manager. In third tier processing, the Program Security Manager does not adjudicate the application, but sends the PAR on to the applicant's appropriate CAF for adjudication. However, not all agencies participate in the tiered approach: the Air Force, NASA, and DARPA do participate, but the Navy does not recognize

tier one, and sends all its PARs to a Program Security Officer for review.

Numerous respondents pointed to SAPs as resistant to reciprocity to varying degrees, many even for visits. Despite the patient efforts by committees to identify and promote uniform procedures, informants noted that SAP personnel understand their programs to occupy extraordinary levels of access defined in good part by themselves. Lack of trust of the judgments of others in the face of these severe security demands means that SAPs seem unlikely to achieve complete reciprocity.

Suitability vs. Security Issues. Whether a person has the skills and personal qualities that make him or her suitable for employment in a certain job, and whether that person's past life and behavior support eligibility for a security clearance and access to classified information, would seem to be separate decisions. One respondent who participated in crafting E.O. 12968 asserted that ideally the two decisions should be taken sequentially: a person is deemed suitable for employment with one set of procedures conducted by human resources personnel, and then he or she is investigated and adjudicated for a clearance by security personnel. The executive order states in Section 2.1 that determinations of eligibility for access to classified information "are separate from suitability determinations with respect to the hiring or retention for employment by the government or any other personnel actions" (E.O. 12968, 1995, Section 2.1 [a]). Decisions on suitability for hiring remain the prerogative of the agency, and reciprocity policy applies only to the second decision on security.

In practice, however, the perceived security demands of various agencies blur this distinction. At Treasury, respondents reported that their agency "religiously" recognized reciprocal access with other agencies, except for certain positions in the Bureau of Printing and Engraving that involved handling large amounts of cash. Those sensitive jobs would require additional screening. Both NSA and CIA noted that the particularly sensitive work of their agencies demanded security eligibility as a condition of suitability for employment—the distinction between suitability and security disappear when covert intelligence and analysis of SCI are the nature of the work. This issue defines a "fault line" mostly running between the IC and the other federal agencies. The fault line divides the IC's use of the polygraph as a standard additional screening procedure from other federal agencies' relative lack of reliance on polygraph testing. It is a fact that complicates achieving reciprocity across the whole spectrum of the federal government. It is one of the arguments for recasting the expectation of reciprocity into a more nuanced policy, in which more complete reciprocity would be expected among IC agencies, but less—or different kinds—of reciprocity, would be expected between the IC and other federal components that exist on the other side of this fault line.

Consequences of Lack of Reciprocity

Respondents agreed on the adverse impact that a lack of reciprocity has on procedures: inefficiency, waste of time, waste of money, and loss of talent. At the DOS, personnel in three distinct offices may need to review a current investigative file before an already cleared person can be hired: Human Resources, Security, and the Bureau of Intelligence and Research that handles SCI for State. Two security officers for an industrial contractor reported that they had each recently undergone a PR by OPM, and they had been required to fill out three different sets

of paperwork, one each for NRO, NSA, and CIA. Many respondents complained about the waste of the government's money if a previously cleared person were being re-investigated by a different government agency at $2,000 to $3,000 per SSBI. Many respondents complained about the time loss suffered by delays, waiting for prior investigative files to be procured and reviewed, waiting for signatures to be obtained on updated forms every 90 days for SAPs, waiting for additional credit and fingerprint checks to come back. Contractors reported that new hires waiting for security clearances to begin their work were a drain on the company's overhead. Government agencies reported that they lost talented applicants seeking to transfer because the delay in processing clearances caused them to go elsewhere. The costly redundancies that critics have been pointing out for 40 years as the consequences of a lack of reciprocity still plague the personnel security system in 2004.

Respondents explained that it typically took 30 to 60 days to get a prior investigative file from DSS, although in the recent past that agency has moved to scanning many of its investigations and transmitting them as electronic files.[16] DOJ officials estimated it took "weeks and weeks" to have a cleared person's access from another agency re-assigned to Justice. Contractors reported that while "cross-overs," the change of a collateral clearance to an SCI access eligibility, had taken 2 to 3 days in the past, currently it took 2 to 3 weeks at CIA.[17] Some noted that personnel in the CIA security office inflicted more delays since they moved to outsourcing some of their work instead of relying on staff employees who had been able to answer questions based on long experience. Frustration about the lack of reciprocity easily shifted into other complaints about the personnel security system, the most prominent being the inordinate length of time it took to complete a background investigation. Since the focus of this study is on cleared personnel seeking to visit, work, or transfer among agencies, how long background investigations are taking to complete, while annoying, is a different problem.

Reasons for Lack of Reciprocity

The officials consulted in this study were asked why they thought reciprocity was not recognized in practice as widely as executive orders and policy directives mandate. Two themes emerged as the most commonly cited reasons for lack of reciprocity: turf and trust.

Many respondents pointed to a determination to exert ownership over the security clearances and accesses held within agencies. Personnel security decisions are one part of a whole complex of procedures that, within the broadly prescribed standards, government agencies tailor to make them fit the demands of their particular agency. When an agency bestows its trust on an individual, the decision is invested with that agency's backing and reputation; it is "*our* clearance," and being required to accept a decision on trustworthiness made by another agency provokes a protest of "but it's not *our* clearance!" Familiar procedures grow comfortable and take on the weight of age the longer they are followed. In any bureaucracy, change is disruptive

[16] Not all respondents in this study were aware of the most recent procedural improvements adopted by key agencies such as DSS that were addressing the problems raised. Being aware of the current status of shifting procedures is a constant challenge across the many and varied agencies, and the lag in awareness can perpetuate undeserved reputations that in turn undermine trust.

[17] The term "cross-over" is used in various ways. Another respondent explained it as eligibility from one agency being accepted by another and the second agency issuing its own clearance to the individual, which would seem to describe a conversion.

and is to be resisted unless it comes from within one's own agency authority structure. Some agencies delay moving from their own methods to standardized procedures long after the latter have been mandated. "Turf control battles are still prevalent on issues of personnel security procedures among SAPs and with SCI," one respondent, who is not from either of those camps, explained.

Virtually all respondents agreed that there is a certain lack of trust based on fear beneath the lack of complete reciprocity. Lack of trust is a symptom of the same structural reality that produces "turf battles": the federal government comprises many agencies and departments with specialized functions, and while at ultimate levels all are trying to work together for the welfare of the country, that still leaves many lesser levels at which competition and the self-interest of one's particular agency can operate. People trust what is familiar and what they can control or at least influence, and distrust what is less familiar and what they cannot control (Kramer, 1999). Investigations done by *our* people, and adjudications made by *our* adjudicators, who have a track record with us and can be confronted if necessary, seem trustworthy. Investigations done by the group across town and adjudicated by that other agency, even though they work with the same prescribed standards of judgment, seem less trustworthy. In one informant's view, how reciprocity actually works is less about applying uniform standards and more about whether someone trusts the people doing the investigations and adjudications.

The fear beneath the lack of trust is not misplaced. It is the fear of making a mistake in judgment and allowing someone access to sensitive information who then betrays his or her trust and damages the security of the United States and the reputation of the agency betrayed. Each espionage incident is a failure to be lived down with redoubled efforts not to fail again, and especially not to fail in the same way again. Because people take seriously the responsibility to protect the information entrusted to them, they try to whittle down the risk of such a failure as small as they possibly can. One informant said, "People do redundant checks because they cover their backs, because of the fear of something happening since the last check, and being caught on their watch." Many respondents mused about how the various communities could—and whether they should—move beyond paralyzing caution to the stance of "risk management" that was written into the executive orders issued in the mid-1990s (E.O. 12958 and E.O. 12968).

Respondents pointed to two interrelated problems that they thought serve as barriers to reciprocity. Some felt stymied by what they perceived as the lack of "uniform, community-wide standards for background investigations." Although supposedly uniform standards have been outlined since 1991 with the SSBI (in NSD 63), and have been refined in executive orders, implementation directives by DoD and other agencies, and policy guidelines on uniform investigations from the SPB, still respondents pointed to variations, differences, and idiosyncrasies they have experienced in background investigations that lead them to distrust. The chronic budgetary and managerial problems that plagued DIS/DSS, and which crystallized in the late 1990s through its ineffective reinvention efforts, caused serious question about extending reciprocity to clearances based on its investigations. Respondents repeatedly noted that they could not trust DSS investigations. Others were reluctant to accept adjudications made by other agencies, usually specified agencies, because they felt the uniform adjudication guidelines were not being applied uniformly. They cited instances of behavior by applicants that was cause for refusal at one agency but would receive a waiver and acceptance at another agency. Respondents

at one IC agency expressed their unanimous opinion that the greatest barrier to reciprocity even within the SCI community was "consistency, that is, the consistent application of the investigative and adjudicative standards" by all segments of the community. Since background investigation and adjudication are the basic processes of the personnel security system, the specific issues respondents raised about these elements offer insights into the day-to-day limits that are placed on reciprocity.

Issues with Background Investigations. As outlined above in the Background section of this report, the creation of DIS in 1972 was intended to standardize DoD background investigations by making one agency responsible for performing the lion's share of them. Agreement on the SSBI in 1991, and the framing of uniform investigative standards in 1997, took two more major steps toward the goal of standardization because they mandated a common investigation for TS and SCI and then common standards for all background investigations done for access eligibility by any federal agency. However, as described by the informants in this study, there remain a multiplicity of federal agencies investigating the backgrounds of their potential employees and contractors.

Within the Treasury Department, for example, the Internal Revenue Service, the U.S. Secret Service, the Customs Bureau, and the Bureau of Alcohol, Tobacco, and Firearms each investigates its own people under a waiver from OPM; the Bureau of Printing and Engraving does its own suitability investigations because of its special mission that exposes people to the temptations of large amounts of cash; and OPM does the investigations needed on the rest of Treasury personnel.[18] The DOS also performs its own background investigations from its field offices, using its own contract investigators as well as a private sector vendor. NSA, CIA, and FBI each perform background investigations on its own agency personnel, and do not automatically accept an investigation done by either of the others. The many personnel assigned to NRO for specified tours of duty are the subjects of SSBIs and SSBI-PRs by an NRO contract investigative agency, except for CIA employees, whose investigations are done by CIA investigators or the contract investigators working for CIA. As suggested above, in October 2003 DoD planned to discontinue DSS's investigative mission and to utilize OPM for all DoD background investigations. Since OPM, in turn, contracts with various private companies for investigations, this move would mean that multiple private companies would actually be performing DoD investigations.

How does it affect reciprocity among agencies if 10 or 20 or 40 different agencies and private companies perform background investigations, as long as all of them are using the same uniform federal standards for background investigations? One impact stems from variations in the procedures used that are apparent among different investigation providers. This study could not focus on details of the procedures used by various investigation providers, but respondents did point out variations that raised concern and diminished reciprocity. (A series of studies is planned that will enable more systematic comparison of the quality of investigations, and this should begin to address the issue of variations among the procedures of providers.) (Youpa,

[18] With the reorganization that accompanied the creation of the Department of Homeland Security (DHS) in 2002, the U.S. Secret Service, the Customs Bureau, and the Bureau of Alcohol, Tobacco, and Firearms moved from the Department of the Treasury to the new DHS. This statement reflects earlier procedures in effect at the time interviews were given.

Marshall-Mies & Carney, 2003). One agency prefers to receive narrative reports on the results of an investigation in order to be able to follow the logic of the judgments that were made rather than see check lists; another discounts interviews that take place over the telephone because they generate less information than face-to-face encounters. Check lists of results and telephone interviews, however, are examples of expedients that have been taken by agencies hard pressed to increase efficiency. DSS, for example, faced a demand for over 500,000 DoD investigations in 2002, and had to find ways to stretch its finite resources.

Agencies that deal with a few hundred or a few thousand investigations per year are less pressed to adopt expedients to achieve efficiency. E.O. 12968 establishes minimum investigative standards that all agencies must meet, but agencies that can afford it may do more than the minimum. CIA and NSA, for example, require that their applicants undergo psychological testing as well as a polygraph test. There are wide disparities in the funding devoted to background investigations among agencies in the various communities that are nevertheless all supposed to reciprocally accept each others' investigations. People are aware that some agencies do the minimum and others invest in additional procedures and personnel. The impression is widespread that not all background investigations are alike, and that there is a hierarchy of quality among them.

A second impact on reciprocity from having an assortment of investigation providers is the variation in the standards for skills and experience of the personnel who perform investigations. There are no uniform personnel standards for investigators.[19] Some agencies cross-train their personnel specialists as investigators, adjudicators, and counterintelligence analysts and rotate them among these assignments, allowing the variety of experience to enrich each of the functions. Others seek retired military intelligence or criminal investigators for the job of background investigator in order to rely on the seasoned judgment such people bring. Private investigations companies may compete with government agencies for personnel with these backgrounds, or they may hire much younger generalists and train them in the specific procedures required. Levels of education, levels of competence in writing reports, relative experience on which to make judgments about people, diligence in tracking down leads and nailing down issues—the standards used for all of these vary among the people hired by different investigation providers.

A third impact stems from an increasing reliance on private companies to do the work of background investigations. Outsourcing is attractive to government agencies because it offers a product for a specified price, while the company takes on the functions of hiring, supervising, and providing benefits for the personnel. However, usually the government agency still must rigorously define its requirements in its contract with the provider, monitor the contractor's procedures, and evaluate the product it receives. The work moves from doing investigations to doing contract monitoring. Whether the amount of work declines is not clear. What is clear is that if contract monitoring by a government agency is ineffectual, the quality of the background investigations produced for the agency can decline. When other agencies review investigative reports done by contractors that seem incomplete or ambiguous, a reputation built on the

[19] See the following section of this report, "Issues with Adjudication," for a brief description of work in progress by the Joint Security Training Consortium to address uniform standards for investigators, adjudicators, and other security personnel.

underlying skepticism about contractors as self-interested, not disinterested, gets planted that is hard to overcome. Respondents repeatedly pointed to instances of inferior investigations that they knew about by this or that contract provider. The accuracy of these perceptions was not as relevant for this study as the fact that, once established, such perceptions generated reluctance to reciprocally accept eligibility determinations without doing more checking themselves. On the other hand, other respondents reported that their agencies were pleased with the quality of investigations from their contract providers and that they had relied on them for years.

Issues with Adjudication. As discussed in the previous background section, consolidating adjudication in DoD from thousands of separate offices into CAFs had been a long, hard-won process that in 1993 resulted in the current configuration of 10 CAFs. Adjudication in non-DoD federal departments such as State, Treasury, or Justice, and among the agencies in the IC, is done by designated offices within those departments. The argument is made that an in-house, or at least departmental, adjudication facility provides necessary convenience, responsiveness, and attention to the particular mores and personnel security needs of an agency, and this line of thought has prevailed over efforts to centralize adjudication further. Thus, although there are uniform Adjudicative Guidelines mandated in E.O. 12968, they are still applied by numerous adjudication offices across the government.

Is this multiplicity a source of inconsistency that impedes reciprocity between agencies? Many respondents thought so. They pointed to cases they (or their adjudicators) had reviewed from other agencies in which varying standards of judgment were apparent in the application of the guidelines. A person favorably adjudicated elsewhere was found to have 11 prior arrests for Driving While Intoxicated (DWIs) and an outstanding arrest warrant in his file; another cleared officer was delinquent to the IRS for $30,000 and had foreign connections that had not been resolved by the previous investigation. A third cleared individual was found to have close relatives imprisoned in a Middle Eastern country on charges of espionage for the KGB, but there was no mitigation of this mentioned in the file. All these examples happen to be of initial adjudications at Military Service CAFs, and they do illustrate a pattern among the respondents interviewed for this study.[20] Among the officials we spoke with, several agreed that military CAFs granted more waivers and more conditional clearances than other DoD CAFs, and that this led to their applicants receiving special scrutiny before reciprocal access would be granted. An OJCS official noted that during the most recent month, 3 out of 10 nominees had to be returned to their parent Service as unfit for assignment to OJCS despite already having been cleared by their Service CAFs. An overall return rate from the OJCS office was estimated at 5 percent. Issues that would typically cause these rejections include financial irresponsibility, foreign connections, alcohol abuse, and emotional problems.

Other respondents pointed out that within an organization, the location at which adjudication is placed affects how the uniform guidelines are applied. At NSA, adjudicators are special agents, cross-trained in investigations and other counterintelligence procedures. The Navy CAF, on the other hand, is located in the Navy Criminal Investigative Service (NCIS); in

[20] We were unable to include interviews with officials at the CAFs of the Military Services in this study, so their perspectives and problems are not reflected in this discussion. It would be unfair to generalize about the quality or patterns of decisions by Service CAFs on the basis of the views of these interviewees without taking a wider sample of opinion.

the view of one respondent, this organizational location tends to impart a law enforcement perspective.[21] Among the people interviewed for this study, those from CAFs responsible for applicants from several different parent CAFs, such as the OJCS or DIA, were most likely to raise discrepancies in judgment patterns or inconsistencies, since they have several adjudicative sources to compare.

Although the goal that led to E.O 12968 was a system-wide application of one set of adjudicative guidelines, few agencies were as unconditional as respondents from the Treasury Department. They reported that no additional investigation would be undertaken on an individual coming from another agency with a current, valid clearance. Military CAFS within DoD are not allowed to re-adjudicate a decision made by another DoD CAF. Allowed the opportunity to make an adjudicative decision for themselves, most agencies interviewed did take that opportunity rather than rely on judgments made elsewhere.

Many respondents thought there is an urgent need for more and different training for adjudicators. Several proposed that if standardized training were developed that adjudicators throughout government could take, this would address the problem of inconsistent application of the guidelines and discrepancies among various agencies. The work currently being done by the Joint Security Training Center (JSTC) to define professional standards for security professions may eventually address this issue, but this work was not yet widely known among respondents interviewed in this study. The low profile may reflect the fact that during the months interviews were being conducted, JSTC was just getting started on its program. The goals of the JSTC research are to standardize and regularize the various security professions across the government. Thus far in the on-going work, they have developed baseline definitions of the security professions. These identify component disciplines, functions, and tasks of each of seven distinct security disciplines, which include background investigators and adjudicators. Building on previous work begun under the SPB, JSTC is identifying and validating skills standards for the various security roles, specifying educational as well as general skills needed to perform these jobs. This effort promises to address the need for standardized training of adjudicators by articulating what adjudicators, as well as investigators, typically do and should be able to do and thus what their training should include (Tippit, Rizzoli, Baker, & Miller, 2002).

In particular, officials at NRO urged that more frequent and higher quality training should be offered to adjudicators government-wide. They described a quarterly interagency forum NRO had been hosting for SCI adjudicators in which people could discuss complex cases and try to build standards of judgment in common. As long as adjudication is done by multiple agencies, expedients such as standardized training, standardized qualifications for adjudicators, standardized placement of the adjudication function within agencies, and discussion round-tables to promote shared judgment are all steps toward the elusive goal of consistency.

Implications

The policy of reciprocity touches on numerous facets of the workings of the personnel security system and the interrelationships between different agencies and departments of the

[21] Another respondent disagreed, however, arguing that DONCAF and NCIS were only linked administratively, not in outlook.

executive branch. Although reciprocity has been a vision held by some in government for decades, progress toward consolidating the three functions affected by reciprocity—investigation, adjudication, and records maintenance—only reached the point in the mid-1990s where reciprocity could be mandated and since then gradually implemented. The findings in this study suggest that the current state of reciprocity is mixed.

When asked to declare whether or not reciprocity was now a problem, respondents split on the answer: half said it was, half said that it really wasn't. However, this seemed to reflect the "glass half full" or "glass half empty" viewpoints of the respondents. When asked for specifics, people in both camps generally agreed that reciprocity was more successful and more widespread in 2003 than it was in 1993. They agreed that collateral-level reciprocity is much improved compared to the past, although it is not perfect. They agreed that within DoD reciprocity had improved. They agreed that visits between agencies or by contractors now can be accomplished more smoothly than in the past, that the Community Badge has improved and simplified routines for visits, and that among IC agencies, SCI reciprocity has also improved.

On the other hand, most respondents agreed that despite the publication of uniform standards for background investigations, uniform guidelines for adjudication, and the imminent achievement of widely available databases to check the status of current clearances, there really were not common criteria followed across agencies of the federal government. There are not consistent procedures followed by various providers of background investigations; there are not common standards for the training of adjudicators or for their application of the Adjudicative Guidelines. Respondents speculated that perhaps it is just not possible to achieve common criteria for these judgment-driven decisions while trying to implement them from a multiplicity of offices. Given the distributed legal authorities over security and intelligence that are in place, and the diversity of missions and constraints among the many agencies encompassed by the reciprocity policy, what we have may be all that can be achieved. Many respondents pointed to the expedients of waivers, conditions, and interim clearances as hindrances to reciprocity because they depart from the agreed-upon standards for everybody. New initiatives such as the Phased PR in DoD, or the passage of the Smith Amendment, were identified as qualifiers on reciprocity no matter how necessary they seemed in the context from which they emerged. Others, especially in industry, pointed to the independence of SAPs to impose their own security requirements for accesses as the more pressing failing of reciprocity because they cause redundant procedures and delays. One official said what we have now is "semi-reciprocity," but because the personnel security system continues to come in for criticism for taking too long to put reliable people into their jobs, there continues to be interest in working toward more complete reciprocity.

Although this issue was not raised directly by the interviewers, lying just beneath the surface of some of the interviews done for this study was skepticism about the necessity for complete reciprocity that is assumed in E.O. 12968. The advantages of standardized and centralized personnel security procedures—benefits such as reducing costs by eliminating duplication and redundancies while increasing efficiency—have beguiled reformers for decades. Security professionals, however, also pointed out to us that there can be disadvantages to complete reciprocity across the various federal agencies, and that these account for some of the less-than-reciprocal practices that are outlined in this report. Respondents who questioned the

basic premise of current reciprocity policy—that the goal is to move toward complete reciprocity—cited several downsides to making reciprocity any more complete than it already is.

Among the problems raised was a potential decoupling of accountability for security from the human judgments inevitably made in vetting procedures. In this view, an agency responsible for the security of information in its care must be able to review, augment as it deems necessary, and exercise its own judgments on the reliability of personnel coming into the agency who need access to its information in order to exercise its accountability. Thus, requesting the file of an existing background investigation for review, and possible further investigation and re-adjudication, is seen as a prudent second look by a new set of eyes—a second look that is likely to enhance the quality of the decision and therefore the level of security. To respondents who argued that complete reciprocity should not be the government's goal, the distinctiveness of agencies in the IC is more significant than the presumed benefits of standardization. The sensitivity of IC sources, the career commitment many IC professionals make, and the level of scrutiny into their personal lives that they accept, all seemed to these respondents to make the IC fundamentally different from agencies that rely on collateral clearances. "Why should we be trying to make reciprocal the background investigations done on the many thousands of 18-year-olds coming into the military in DoD who need Secret clearances, with those done on several hundred applicants to an IC agency who are offering to spend their careers in intelligence work?" one respondent asked, summing up this view. Like the driver's license reciprocity described in the introduction of this report—complete in the short term but partial in the long term—these respondents argued for changing the policy to a more nuanced reciprocity that recognized differences among the communities.

Options for Action

What, if anything, can and should be done about reciprocity? The following options structure the opinions of respondents and the implications that emerged from doing this study and thinking about these issues.

1. Continue Doing More of the Same

Some respondents thought it best not to tinker further with the policies, authorities, and procedures affecting reciprocity. This group divided between those who were fatalistic and thought the current "semi-reciprocity" was probably all that could be achieved given the "turf and trust" issues discussed above, the real distinctions between agencies, and the new demands the terrorist attacks have forced on the country; and those who were optimistic and thought the work of on-going interagency committees, initiatives by OSD, and the slow but steady implementation of agency-level reciprocity directives would continue to improve reciprocity enough so that additional reforms will be unnecessary.

Not undertaking major initiatives on reciprocity at this time has obvious advantages. It is the least disruptive course, and it demands the least time and energy from individuals who are already busy. It assumes that current ways of doing things and dealing with reciprocity will continue, with at least marginal improvements gained over time by the work of committees like

the Personnel Security Working Group[22] or the NISPPAC (Information Security Oversight Office, n.d.) both of which continue to work on coordination of reciprocity issues. It reflects the judgment of those respondents who felt that reciprocity is no longer the most pressing issue faced in personnel security, and that reciprocity is "pretty good," now, or at least that it is "good enough."

This approach also puts emphasis on and hope in increasing reciprocity in defined arenas. OSD has worked steadily to sponsor procedures to systematize SAPs within DoD into acknowledged, unacknowledged, and waived SAP sub-communities, with base procedures for each outlined in the Overprint to the NISP Supplement. The IC agreed almost unanimously to follow an MOA on standards for the polygraph that has helped to systematize polygraph policies. Many respondents were hopeful that impending achievements in electronic databases, including JPAS, CVS, and Scattered Castles, would remove many of the delays and annoyances over checking current clearance and access statuses. The efforts of the JSTC to define skills standards for professional security roles promise to support the development of more standardized training for adjudicators as well as investigators. The achievement of more reciprocity within communities or within arenas is a real achievement even if it is partial, and even if it leaves unsolved some other issues of reciprocity between communities. As the driver's license analogy discussed in the introduction above suggests, reciprocity does not necessarily imply unconditional or complete transferability.

The disadvantage of this option for those with the vision of far-reaching reciprocity is that it acknowledges that a uniform, consistent government-wide personnel security system is probably not going to be realized.

2. Try Money

Some respondents felt that a disparity in the funding devoted to personnel security programs by the various agencies seriously hinders reciprocity. One individual, whose agency enjoys ample resources, felt that DoD (the largest agency in terms of personnel) systematically under-funds personnel security and expects more for less. In this individual's view, DSS investigators had too many cases to handle to be able to do a good job on them. "You get what you pay for," he said, "DoD hasn't put their money where their mouth is when it comes to personnel security." NSA, for example (a DoD agency with IC status), assigns two adjudicators to each case in order to ensure a judgment is reached from different points of view. NSA tried using check lists in their investigative reports as a cost-saving measure in the mid-1990s, but abandoned them as too superficial a few years later and went back to the more labor-intensive and costly narrative format. DoD check lists in investigative reports came in for criticism from numerous respondents. Another respondent had decided that because of the lengthening delays in completing background investigations by DSS and the backlog of DoD adjudications (both of which could be at least addressed by devoting more resources and personnel to them) the CAFs were accepting investigations that were incomplete or had unresolved issues in order to move the mountain of cases along. An official from another agency generalized that his agency found DSS investigative files to be incomplete or not properly expanded, so his agency expended its own

[22] The current PSWG is a subcommittee of the Records Access and Information Security Policy Coordinating Committee of the National Security Council.

investigative resources to follow up on the issues they found in files. A third respondent pointed to "DoD cost–cutting" as one of the main factors in other agencies losing confidence in DoD adjudications and consequently stepping back from reciprocity.

Another respondent noted that, in his wide experience, security departments typically lack the resources they need, and they are handy targets for cost cutting, because security is auxiliary to the mission of most agencies. In contrast, intelligence agencies, which cannot do their work without the most rigorous personnel security and for whom suitability and security determinations merge, do allocate adequate resources to personnel security functions. Without adequate resources, people do not respect the work of security, and without respect it is even harder to make a convincing case of the need for more money. Industrial contractors can short-change security even more than government, in this person's view, because they demand that security not interfere with efficiency of operations that ultimately makes the money for the company. A sense of stepping into a morass accompanies these observations: complaints about timeliness of investigations put pressure on investigators for efficiency, while complaints about the quality of the resulting investigations create pressure for spending more time and effort on leads and narrative reporting. Complaints about backlogs in adjudication decisions put pressure on adjudicators to be more efficient, while complaints about unresolved issues found in the resulting adjudicative files create pressure for spending more time on cases, spending more money on training, or devoting more people with higher levels of education to the adjudication function. There is well-earned skepticism that throwing infusions of money at any problem will necessarily solve it, but if the essential backing for it can be developed, this long-running problem in DoD of under-funding personnel security may be a good candidate for more funding.

The recommendation made by several respondents that a standardized training program in adjudication be developed that could be available to adjudicators across federal agencies would be one initiative dependent on additional resources. Another would be the funding of a suggestion to do more frequent, higher-quality training cooperatively across the IC in order to develop common approaches to application of the Adjudicative Guidelines.

3. Restructure the Context for Reciprocity

Some respondents expressed frustration with the inability of "some overarching Governmental authority to impose the reciprocity standards in E.O. 12968 on the rest of the government." As has been characteristic of personnel security policy (and perhaps of many other federal policies), new initiatives like reciprocity in the 1990s have been overlaid onto existing policies without a complete reworking and integrating of the old and the new. Major changes are so disruptive, so difficult to achieve agreement by the various existing authorities, and so complicated to craft, that smaller incremental change that leaves familiar structures in place is almost always the approach chosen. E.O. 12968 was a compromise that mandated far-reaching reciprocity, but it left in place elements that worked against achieving it: the DCI's responsibility for and the control over SCI; the prerogatives and responsibilities delegated by the DCI to the designated SOICs for safeguarding SCI in their respective agencies; the two streams of policy defining differing standards that descend from DCIDs and from DoD directives; and the caveat that an agency must be able to satisfy itself that nothing at issue has changed since an individual's last investigation before it accepts an adjudication from another agency. These have

proven unsteady pillars on which to support a reciprocity policy.

As an informant from a large industrial contractor noted, since SOIC authority gives each SOIC agency head control over the SCI it uses, each assumes the risk along with the control. Each tries to "own" the users of the information who could abuse the agency's trust. Distributed responsibility for risk leads to attempts at turf control and reluctance to trust judgments not made under that agency's auspices. Reciprocity policy minimizes the distinctions between the IC, DoD, and the other federal agencies each with its own missions and features. In practice, the distinctions have asserted themselves and have forced work-arounds, expedients, and compromises that have allowed the system to work at all. Since 1997, persistent difficulties at DSS generated backlogs and provoked skepticism in other federal agencies about DSS products, and these developments coincided with the period that the strongest reciprocity policy has been in place. Perhaps troubles at DSS prevented reciprocity from being played out more smoothly, or perhaps the underlying bureaucratic incentives did more to defeat the vision of uniform reciprocity.

Some respondents felt there has been a waning of enthusiasm and support for government-wide reciprocity. The dissolution of the SPB in 2001 was seen as a symptom of this loss of motivation to push for yet a higher level of reciprocity, and its loss was singled out, especially by industry respondents, as the loss of a forum that had been valuable for discussing and resolving reciprocity problems. The new context imposed by the terrorist attacks in 2001 and the consequent creation of the DHS and realignments within the FBI and CIA to better analyze terrorist threats now may all focus attention and energy on immediate dangers, and less on efficient interaction among agencies on personnel security. The time to restructure the basic authorities that underlie the personnel security system and its reciprocity policy may not be at hand. When frustration with the lingering residue of inconsistencies and the wasting of time and energy builds up again, another advocate for reciprocity may step forward. If so, he or she should consider the necessity of restructuring the context of laws, executive orders, and agency directives to support reciprocity better.

4. Eliminate the Need for Reciprocity by Consolidation

Suggestions from study groups that urge consolidation of personnel security date back decades. To these groups it seemed obvious that the federal government should create a single organization to do background investigations and a single organization to do adjudication and a single database accessible to anyone checking clearance status. Such a radical move holds out to these visionaries the tantalizing gains of consistency, uniformity, accountability, and simplicity. They would emphasize the essential similarities of the three functions of personnel security no matter which agency performs them, and thereby they would deemphasize all the idiosyncrasies and special needs and ways of doing things that loom large in people's experience with the actual functioning of any agency (General Accounting Office, 1995).[23] When the PERSEREC study on

[23] When the GAO studied possible consolidation of investigations and adjudication in 1995, GAO staff contacted 51 federal agencies. They reported that 34 out of 51 agencies, and 8 out of 9 key agencies, opposed further consolidation of adjudication. Six of nine key agencies also opposed further consolidation of investigation providers, but three (DoD, OPM, and DOE) favored it. Reasons for opposition followed many of the points discussed here, reiterating the unique missions and needs of particular agencies.

consolidating CAFs recommended a single DoD CAF in 1991, that proposal was rejected in favor of 10 agency-centered CAFs (Crawford, Riedel & Carney, 1991). When the JSC made an impassioned case for a single investigative agency in 1994, that proposal was rejected, and with the proposed move of DoD investigations to OPM and the accompanying shift to more contractor investigations, the pattern of investigation providers for the future seems to be moving toward multiplicity, not consolidation. While there has been progress since 2000 in consolidating data for records maintenance into electronic databases such as JPAS, CVS, and Scattered Castles, no one is expecting that these will merge into one entity. Backers for the consolidations that would provide the bases for real reciprocity are nowhere in sight, but shifts in demands for personnel and frustration with the current system's failings could create them.

5. Redefine Reciprocity to Reflect Differences between the IC and Other Agencies

Some respondents from the IC stressed that the investigative standards in E.O. 12968 are only minimums and that agencies are explicitly authorized by the order to undertake additional procedures as they deem necessary to meet their responsibilities. The special character of the intelligence the IC develops and uses, the career patterns of many of its employees, and the comparatively well-funded operations of its personnel security program that underwrite techniques such as the polygraph and psychological testing, support the views of these respondents that the IC agencies are irreducibly distinctive. These respondents argue that reciprocity among IC agencies profitably could be developed further, but that reciprocity between the IC and non-IC agencies should be redefined to acknowledge these distinctions. From their perspective, complete reciprocity should not be the goal of the federal government. Following this line of argument would mark a retreat from the reciprocity policy enunciated in E.O. 12968 toward a nuanced, conditioned approach reminiscent of the policies on driver's licenses.

Table 1
Summary of Main Points about Reciprocity

What works quite well	• Visits • Community badge • Updating the SF-86
What sometimes works	• Electronic databases • Reviews of prior investigations • Polygraph reciprocity
Expedients adopted to make things work that affect reciprocity	• Interim clearances and accesses • Waivers
What works imperfectly	• Conversions of clearances and accesses • Reciprocity for industrial contractors • Reciprocity among SAPs • Suitability vs. security issues
Consequences of lack of reciprocity	• Examples of waste of time, money, talent
Reasons for lack of reciprocity	• Ownership of the access • Trusting the other's judgment and procedures
Issues with investigations	• Multiple and differing providers perform investigations; uniform investigative standards are minimums; there are no uniform qualifications for investigators; more investigations are outsourced to contractors.
Issues with adjudication	• Multiple agencies do their own decision-making; adjudication offices are placed differently within organizations; there are differing training and qualifications for adjudicators; there is a need for more and standardized training of adjudicators.
Implications	• Reciprocity is improved but not complete; now it is semi-reciprocity; should the government be trying to achieve complete reciprocity?
Options for Action	• Continue doing more of the same • Try money • Restructure the context with the SOICs • Eliminate the need for reciprocity by consolidating • Redefine reciprocity between IC and non-IC agencies

References

Aftergood, S. (2002, April 10). Security chasing its tail. *Security News, 2002 (29)*. Retrieved October 26, 2002, from http://www.fas.org.html

Berger, S. (1997, March 24). Implementation of Executive Order 12968. Memorandum from the Assistant to the President for National Security Affairs to George J. Tenet and John P. White, Co-Chairmen, Security Policy Board.

Blue Ribbon Defense Panel. (1970). *Report to the President and the Secretary of Defense on the Department of Defense*. Washington, DC: Author.

Bush, G.H.W. (1991, October 21). National Security Directive 63, *Single scope background investigation.*

Carney, R.M. (1991). *Evaluation of the productivity of the special background investigation.* Monterey, CA: Defense Personnel Security Research Center.

Carney, R.M. (1996). *SSBI source yield: An examination of sources contacted during the SSBI.* Monterey, CA: Defense Personnel Security Research Center.

Clinton, W.J. (1994, September 16). Presidential Decision Directive 29, *Security Policy Coordination* (For Official Use Only).

Code of Federal Regulations. (2002). Title 10, Subtitle A, Part IV, Chapter 134, Subchapter I, Sec. 2244. National Archives and Records Administration Office of the Federal Register. Washington, DC: U.S. Government Printing Office.

Commission on Protecting and Reducing Government Secrecy. (1997). *Secrecy: Report of the Commission on Protecting and Reducing Government Secrecy* (Senate Report 105-2). Washington, DC: U.S. Government Printing Office.

Crawford, K.S., Riedel, J.A., & Carney, R.M. (1991). *Consolidation of personnel security adjudication in DoD.* Monterey, CA: Defense Personnel Security Research Center.

Department of Defense. (1982, April 16). *Select panel review of the Department of Defense personnel security program* (For Official Use Only).

Department of Defense. (2003, January 24). (Management Initiative Decision 908), *Reengineering the Personnel Security Program.* (For Official Use Only).

Department of Defense Inspector General. (1997). *Personnel security in the Department of Defense* (Rep. No. 97-196). Washington, DC: Author.

Department of Defense Industrial Review Committee. (1984). *Analysis of the effectiveness of the Department of Defense industrial security program and recommendations for program*

improvement. Washington, DC: Author.

Department of Defense Inspector General. (2001). *Defense Clearance and Investigations Index database*. Washington, DC: Author.

Department of Defense Personnel Security Working Group (PSWG). (1974). *A review of the Department of Defense Personnel Security Program, 1974* (For Official Use Only). Washington, DC: Author.

Deputy Secretary of Defense. (1994). Special Access Program Oversight Committee. *Information Bulletin*. Retrieved October 12, 2003, from http://www.fas.org/spg/othergov/sapoc.html.

Director of Central Intelligence Directive 1/14. *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)*, August 12, 1994.

DoD Directive 5105.42, *Charter for Defense Investigative Service*, April 18, 1972.

DoD Directive 5200.2-R, *Personnel Security Program,* December 20, 1979.

DoD Directive 5200.2-R, *Personnel Security Program,* January 1, 1987.

DOD Directive 5220.22, *DoD Industrial Security Program,* December 8, 1980.

DoD Directive 5220.22-M, *National Industrial Security Program Operating Manual,* January 1, 1995.

DoD Directive 5220.22-M-Sup 1, *National Industrial Security Program Operating Manual Supplement*, February 1, 1995.

DoD Overprint to the National Industrial Security Program Operating Manual Supplement, January 14, 1998 (For Official Use Only).

Eisenhower, D. D. (1961, January 17). Final TV talk. Box 38, Speech Series, Papers of Dwight D. Eisenhower as President 1953-61, Eisenhower Library, National Archives and Records Administration.

Executive Order 10450, *Security Requirements for Government Employees*, April 27, 1953.

Executive Order 12829, *The National Industrial Security Program,* January 6, 1993.

Executive Order 12968, *Access to Classified Information*, August 2, 1995

General Accounting Office. (1981). *Faster processing of DoD personnel security clearances could avoid millions in losses.* Washington, DC: U.S. Government Printing Office.

General Accounting Office. (1995). *Background investigations: Impediments to consolidating investigations and adjudicative functions* (GAO/NSIAD-95-101). Washington, DC: U.S. Government Printing Office.

General Accounting Office. (1999). *DOD personnel: Inadequate personnel security investigations pose national security risks* (GAO/NSIAD-00-12). Washington, DC: U.S. Government Printing Office.

General Accounting Office. (2000). *Weaknesses in security investigation program are being addressed.* Testimony by Carol C. Schuster. Washington, DC: U.S. Government Printing Office.

Gruber, A. (2003, June 4). Online security clearance forms on track for June debut. *Government Executive Magazine.* Retrieved November 3, 2003, from http://www.govexec.com .

Harris, G.R. (1998). *Personnel security reciprocity.* Unpublished paper.

House of Representatives, Committee on Government Reform. (2002). *Defense Security Service: The personnel security investigations [PSI] backlog poses a threat to national security* (Rep. No. 107-767). Washington, DC: U.S. Government Printing Office.

Information Security Oversight Office (ISOO). (n.d.) *The national industrial security program.* Washington, DC: National Industrial Security Program Policy Advisory Committee.

Joint Security Commission. (1994). *Redefining security: A report to the Secretary of Defense and the Director of Central Intelligence.* Washington, DC: Author.

Joint Security Commission. (1999). *Report by the Joint Security Commission II.* Washington, DC: Author.

Kramer, R.M. (1999). Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual Review of Psychology*, pp. 1-33.

National Science Academy, National Research Council. (2002). *The polygraph and lie detection.* Washington, DC: Author.

Nelson, P. R. (2003). *A review of certain historical factors impinging on the development of reciprocal acceptance of security clearances/access in DoD and the federal government.* Unpublished draft.

Peckenpaugh, J. (2003, September 4). Contractor workforce grows as civil service shrinks. *Government Executive Magazine.* Retrieved October 15, 2003, from http://www.govexec.com.

Security Policy Board. (n.d.) *National policy on reciprocity of use and inspection of facilities and guidelines for the implementation,* and *Oversight of the policy on reciprocity of use and inspection of facilities.* Retrieved October 23, 2003, from

http://www.fas.org/sgp/spb/recipro.html

Security Policy Board Forum. (1998). Memorandum of Agreement. Cited in Joint Security Commission (1999). *Report by the Joint Security Commission II.* Washington, DC: Author.

Tippit, J.D., Rizzoli, R.A., Baker, S., & Miller, M.A. (2002). *Baseline definition of the security profession.* Foster City, CA: The Tippit Group.

Youpa, D.G., Marshall-Mies, J.C., & Carney, R.M. (2003). *Development and evaluation of a single scope background investigation quality rating form* (Tech. Rep. 0302). Monterey, CA: Defense Personnel Security Research Center.

Appendix A

Agencies and Companies That Participated in Interviews

1. National Security Agency (NSA)
2. Department of Defense (DoD)
3. Department of Justice (DOJ)
4. Department of State (DOS)
5. Department of Treasury (Treas)
6. Department of Energy (DOE)
7. [Intelligence] Community Management Staff (CMS)
8. Office of the Joint Chiefs of Staff (OJCS)
9. DOD Washington Headquarters Service (WHS)
10. Federal Bureau of Investigation (FBI), and National Security Council staff, retired
11. Personnel Security Research Managers' Program Staff (PSMRP)
12. Central Intelligence Agency (CIA)
13. Defense Intelligence Agency (DIA)
14. National Reconnaissance Agency (NRO)
15. TRW, Inc.
16. The Boeing Company
17. Northrop Grumman Corporation
18. MCA Engineers, Vandenberg AFB, (respondents included a NISPPAC representative)
19. BAE Systems, (respondents included an ISWG officer)

Appendix B

Interview Protocol
Areas for Discussion in Interviews on Reciprocity

1. To begin, could you tell us about your agency's procedures for implementing reciprocity regarding a person who has a current background investigation and clearance from a different organization:

   a) coming to you on a one-day visit that will require access to classified information;

   b) coming to work temporarily on a project that will require access to classified information;

   c) coming to you as a job applicant.

2. How do you implement reciprocity when your agency sends people with access to other organizations: does this differ depending on the organization being exchanged with or the type of organization (IC versus DoD, or DoD versus non-DoD).

3. In effect, what are your agency's bottom-line standards for reciprocity, i.e., what are the key criteria that must be met in order to reinstate a clearance?
   (Possible standards: length of time since last SSBI, length of break in service in government employment, agency that performed the SSBI, agency that adjudicated and granted access).

4. To summarize what you've said, and to check that I've understood correctly, your agency defines reciprocity in these ways _____ ; and implements it in these ways for visits _____, for granting access _____, and for employment _____.

5. Under what circumstances would you request that person's investigative file be sent to you?

   Under what circumstances would you request an updated SF86 and initiate a new background investigation?

6. At your agency, is a polygraph required for reissuing a clearance or SCI access if a person comes with eligibility granted elsewhere?

7. Are you familiar with the Clearance Verification System initiative (part of the larger E-Government project, it offers the opportunity to view current clearance information via the Web) and its potential impact on reciprocity?

   What reciprocity issues, if any, will this system's enhanced connections into PSI databases address for your agency?

8. From your perspective, what are the impediments to a smoothly functioning, seamless reciprocity process? What are the advantages, and disadvantages, for the federal government of having a smoothly functioning reciprocal personnel security system?

9. In order to collect data that can be compared across agencies, we would like to send you three or four brief scenarios that describe in a few paragraphs situations involving reciprocity, and ask you to tell us how your agency typically would respond to them.

   Would you be willing to respond to scenarios?
   Would you be willing to be identified by agency name, or simply by type of community?

10. Who in your agency could we ask about obtaining data relating to reciprocity, such as data on the number of people who come into your agency with clearance needing temporary access, or as job applicants?[24]

11. Who else in your organization should we talk to for their insights on reciprocity or for more information about reciprocity and its impact on personnel security?

[24] The collection of data on actual numbers of people annually affected by reciprocity, e.g., those moving among agencies for various lengths of time as visitors, temporary assignees, or as employees, proved unfeasible. The incompatibility of systems used by personnel departments to define these various statuses, and the incompatibility of electronic databases of personnel records, defeated this part of the study.